Controlled and combined remote implementations of partially unknown quantum operations of multiqubits using GHZ states

An Min Wang*
Group of Quantum Theory, Department of Modern Physics
University of Science and Technology of China, Hefei, 230026, P.R.China

We propose and prove protocols of controlled and combined remote implementations of partially unknown quantum operations belonging to the restricted sets [An Min Wang: PRA, **74**, 032317(2006)] using GHZ states. We detailedly describe the protocols in the cases of one qubit, respectively, with one controller and with two senders. Then we extend the protocols to the cases of multiqubits with many controllers and two senders. Because our protocols have to demand the controller(s)'s startup and authorization or two senders together working and cooperations, the controlled and combined remote implementations of quantum operations definitely can enhance the security of remote quantum information processing and potentially have more applications. Moreover, our protocol with two senders is helpful to farthest arrive at the power of remote implementations of quantum operations in theory since the different senders perhaps have different operational resources and different operational rights in practice.

PACS numbers: 03.67.Lx, 03.67.Hk, 03.65.Ud, 03.67.-a

I. INTRODUCTION

Quantum teleportation [1] is one of the most striking developments in quantum theory. It indicates that a quantum state can be remotely transferred in a completely different way compared with a classical state. Thus, one would like to know whether and how a quantum operation can also be remotely transferred in a completely different way compared with a classical operation. This problem is just so-called the remote implementation of quantum operation (RIO), which was ever studied successfully by Huelga, Plenio and Vaccaro (HPV) [2, 3] for the case of one qubit. Recently, we proposed and proved a protocol of remote implementations of partially unknown quantum operations of multiqubits via deducing the general restricted sets and finding the unified recovery operations [4].

Remote implementation of a quantum operation means that this quantum operation performed on a local system (sneder's) is teleported and it acts on an unknown state belonging to a remote system (receiver's) [2, 3, 4]. Here, a sender is a person who transfers a quantum operation, and a receiver is a person whose system receives this quantum operation and this quantum operation acts on an unknown state belonging to him/her. Obviously, the RIO is different from simple teleportation of quantum operation without action, and it is also not an implementation of nonlocal quantum operation [5, 6], although there are the closed connections among them. Actually, all of them play the important roles in distributed quantum computation [5, 6], quantum program [7, 8] and the other remote quantum information processing tasks. Recently, a series of works on the remote implementations of quantum operations appeared and made some interesting progress both in theory [2, 3, 4, 9] and in experiment [10, 11, 12].

Both HPV's and our recent protocols use Bell states as a quantum channel. However, it is well-known that GHZ states [13] are also very important quantum resource in quantum information processing and communication (QIPC). Just motivated by the scheme of teleportation of quantum states using GHZ state [14, 15, 16] and the fact that it has been successfully applied to quantum secret sharing [17], we would like to investigate the remote implementations of quantum operations using GHZ state(s). Nevertheless, the more important motivations using state(s)in our protocols are to enhance security, increase variety, extend applications as well as advance efficiency via fetching in some controllers and two senders. Our results again indicate that GHZ states are powerful resources in QIPC.

It is useful and interesting to investigate the remote implementations of partially unknown quantum operations because they will consume less overall resource than one of the completely unknown quantum operations, and such RIOs can satisfy the requirements of some practical applications. Here, the "partially unknown" quantum operations are thought of as those belonging to some restricted sets which satisfy some given restricted conditions. In Refs.

---

*Electronic address: anmwang@ustc.edu.cn

[2, 3, 4], the restricted sets of quantum operations were seen to be still a very large set of unitary transformations because their unknown elements take continuous values. In the simplest case of one qubit, two kinds of restricted sets of quantum operations are, respectively, a set of diagonal operations and a set of antidiagonal operations [3]. For the cases of multiqubits, we obtained the general forms of restricted sets of quantum operations and the unified recovery operations, then proposed and proved our protocol of remote implementations of quantum operations belonging to the restricted sets in our recent work [4]. Specially, our restricted sets of quantum operations are not reducible to a direct product of two restricted sets of one-qubit operations, our recovery operations have general and unified forms, and so our protocol can be thought of as a development of HPV protocol to multiqubits systems but not a simple extension of HPV protocol [3].

It must be emphasized that the main advantage using GHZ states in the RIO protocols is to provide ability for fetching in (many) controller(s) or/and more than one sender. When there is(are) the controller(s), we call the remote implementation of quantum operations as controlled one, when there are more than one sender, we called the remote implementation of quantum operations as combined one. A controlled remote implementation of quantum operation has to have the controllers' participation. A combined remote implementation of quantum operations has to have the senders' cooperation. Otherwise, the RIOs cannot be faithfully and determinedly completed.

In the controlled RIOs, not only a controller plays such a role that the quantum channel between sender and receiver is opened by his/her operations, but also the controller's measurement (classical information) impacts the form of the sender's operations or the receiver's operation. This implies that the controller's action contains "start up" and "authorization" so that the RIOs can be faithfully and determinedly completed. Just based on this fact, we can say the controlled RIOs definitely enhance the security of remote quantum information communication and processing. In addition, varying with the ways of authorization by the controller, the steps in RIO protocols have their different forms. It seems to bring about some complicated expressions of our protocols, but aiming at the different cases, the controlling process needs such variety. For example, if the controller trusts in the sender or is easy to communicate with the sender, he/she authorizes to the sender; if the controller trusts in the receiver or is easy to communicate with the receiver he/she authorizes to the receiver; if the controller hopes to keep the "say last words", he/she authorizes to the receiver at a chosen stage of the protocols.

While in the combined RIOs, the later sender has to obtain the classical information from the former one by one in the sending sequence of protocols so that he/she can correctly choose his/her operation. Therefore, the combined RIOs can also definitely enhance the security of remote quantum information communication and processing. Note that the security enhancement is in classical sense, this can be called so-called "sequential multiple-safety". This concept can be understood and illustrated by a classical example of opening safe-deposit box. For simplicity, let us only consider the case of sequential double-safety. This example is how to open a safe-deposit box with two locks and its every lock has a set of various keys. Suppose the set of keys of the first lock are $k_1^A, k_1^B, \cdots$, the set of keys of the second lock are $k_2^A, k_2^B, \cdots$. Opening the safe-deposit box needs to use the sequential and paired keys (k_1^A, k_2^A), or $(k_1^B, k_2^B), \cdots$ to complete it. Otherwise the safe-deposit box can not be opened. In other words, two guardians (corresponding two senders) have to cooperate each other. When the first guardian opens the first lock using some given key k_1^C (corresponding a quantum operation belonging to some given restricted set), he/she has to tell the second guardian his/her using C key so that the second guardian can correctly use k_2^C to open the safe-deposit box. Of course, we can say that the combined RIO has higher security. In addition, in the combined RIOs, our protocol with two senders is also helpful to farthest arrive at the power of RIOs in theory. Actually, since it is possible that different senders have different operational resources and different operational rights in practice, their cooperations can combine more or more suitable operations and then our protocol with two senders has a higher practical power of RIOs than one with only one sender.

Note that in this paper, we only use three partite GHZ states in our protocols. Therefore, we have at most two senders if only using N GHZ states in the cases of N qubits. In fact, when using more than three partite GHZ states, we can further extend our protocols to the cases of more than two senders, even many controllers and many senders together.

Because the no-cloning/broadcast theorem [18, 19] forbids faithfully to transfer an unknown, even partially (un)known quantum operation to two locations at the same time, we give up to consider such a scheme. However, alternatively, we can construct a symmetric scheme among three parties (locations), in which every parter plays a role among sender, receiver and controller in the controlled RIOs, or two parters play two senders and the other parter plays a receiver in the combined RIOs.

Besides Sec. I is written as an introduction, this paper is organized as follows: in Sec.II, we simply recall the RIO protocols using Bell states and introduce our restricted sets of quantum operation of multiqubits; in Sec. III we propose and prove protocols of controlled remote implementations of partially unknown quantum operations of one qubit using one GHZ state; in Sec. IV we propose and prove a protocol of combined remote implementations of partially unknown quantum operations of one qubit using one GHZ state; in Sec. V, by aid of the explicit form of our restricted sets of quantum operations of N qubits [4] and the general swapping transformations, we extend our

protocols to the cases of multiqubits; in Sec. VI, we summarize and discuss our results; in appendixes, we analyze the general swapping transformations used in this paper, and provide the proofs of our protocols in detail for the cases of more than one qubits.

II. RIO USING BELL STATES

In the HPV protocol [2, 3], the joint system of Alice and Bob initially reads

$$\left|\Psi_{ABY}^{\rm ini}\right\rangle = |\Phi^+\rangle_{AB} \otimes |\xi\rangle_Y, \tag{1}$$

where

$$|\Phi^+\rangle_{AB} = \frac{1}{\sqrt{2}}\left(|00\rangle_{AB} + |11\rangle_{AB}\right) \tag{2}$$

is one of four Bell states which is shared by Alice (the first qubit) and Bob (the second qubit), and the unknown state (the third qubit)

$$|\xi\rangle_Y = y_0|0\rangle_Y + y_1|1\rangle_Y \tag{3}$$

belongs to Bob. Note that the Dirac's vectors with the subscripts A, B, Y in the above three equations indicate their bases, respectively, belonging to the qubits A, B, Y.

The quantum operation to be remotely implemented belongs to one of the two restricted sets defined by

$$U(0,u) = \begin{pmatrix} u_0 & 0 \\ 0 & u_1 \end{pmatrix}, \quad U(1,u) = \begin{pmatrix} 0 & u_0 \\ u_1 & 0 \end{pmatrix}. \tag{4}$$

We can say that they are partially unknown in the sense that the values of their matrix elements are unknown, but their structures, that is, the positions of their nonzero matrix elements, are known. In our notation, a restricted set of one-qubit operations is denoted by $U(d,u)$, where $d = 0$ or 1 indicates, respectively, this operation belonging to diagonal- or antidiagonal restricted set, while u is its argument (unknown elements).

The simplified HPV protocol can be expressed by five steps, which is made of Bob's preparing, the classical communication from Bob to Alice, Alice's sending, the classical communication from Alice to Bob and Bob's recovering [4]. The whole protocol can be illustrated by the following quantum circuit: (see Fig.1):

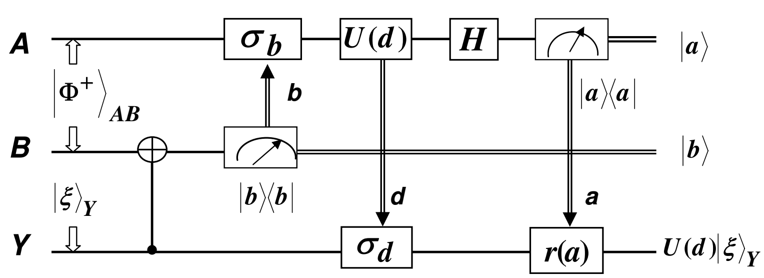

FIG. 1: Quantum circuit of the simplified HPV protocol, where $U(d)$ is a quantum operation to be remotely implemented and it is diagonal or antidiagonal, H is a Hadamard gate, σ_b, σ_d are identity matrices or NOT gates (σ_1) with respect to $b, d = 0$ or $b, d = 1$, respectively, and $r(a) = (1-a)\sigma_0 + a\sigma_3$ is an identity matrix when $a = 0$ or a phase gate (σ_3) when $a = 1$. The measurements $|a\rangle\langle a|$ and $|b\rangle\langle b|$ are carried out in the computational basis ($a, b = 0, 1$). "⇒" (crewel with an arrow) indicates the transmission of classical communication to the location of the arrow direction.

In order to extend the RIO protocol to the cases of multiqubits, we first have to seek for the correct restricted sets of quantum operations of multiqubits that can be remotely implemented in a faithful and determined way. Actually, we have obtained their general and explicit forms in our recent works [4], that is, the restricted sets of quantum operations of N qubits have such forms that every row and every column of operations belonging to them only has one nonzero element. Thus, it is easy to know that there are $2^N!$ restricted sets of operations in the N-qubit systems. Denote the xth restricted set by $T_N^r(x,t)$, and its nonzero element in the mth row by t_m, we have

$$T_N^r(x,t) = \sum_{m=1}^{2^N} t_m |m, D\rangle\langle p_m(x), D|. \tag{5}$$

Here, $x = 1, 2, \cdots, 2^N$ and

$$p(x) = (p_1(x), p_2(x), \cdots, p_{2^N}(x)) \tag{6}$$

is an element belonging to the set of all permutations for the list $\{1, 2, \cdots, 2^N\}$. Moreover, when the requirement of the unitary condition is introduced, t_m will be taken as $\mathrm{e}^{\mathrm{i}\phi_m}$, and ϕ_m is real.

To remotely implement quantum operations belonging to the above restricted sets, the sender(s) needs a mapping table which provides one-to-one mapping from $T_N^r(x,t)$ to a classical information x ($x = 1, 2 \cdots, 2^N!$), and the receiver knows a mapping table which gives out one-to-one mapping from a classical information x ($x = 1, 2 \cdots, 2^N!$) to $R_N(x)$ defined by

$$R_N(x) = T_N^r(x, 0) = \sum_{m=1}^{2^N} |m, D\rangle\langle p_m(z), D|. \tag{7}$$

Obviously, it has the same structure as $T_N^r(x,t)$ to be remotely implemented, and it is an important part in the final recovery operation.

For simplicity, let us consider the case of two qubits. It is clear that there are 24 kinds of restricted sets of quantum operations that can be remotely implemented. In our RIO protocol, we use two Bell states $|\Phi^+\rangle_{A_1B_1}, |\Phi^+\rangle_{A_2B_2}$ as the quantum channel, where qubits A_1, A_2 belong to Alice and B_1, B_2 belong to Bob. Initially, an unknown state $|\xi\rangle_{Y_1Y_2}$ also belongs to Bob. Bob first performs two controlled-NOT (C^{not}) transformation by using Y_1, Y_2 as control qubits and B_1, B_2 as target qubits, respectively. Then he measures his qubits B_1 and B_2 in the computational basis $|b_1\rangle_{B_1}\langle b_1| \otimes |b_2\rangle_{B_2}\langle b_2|$, where $b_1, b_2 = 0, 1$ and sends the results to Alice. After receiving the two classical bits, Alice first carries out the quantum operations $\sigma_{b_1}^{A_1} \otimes \sigma_{b_2}^{A_2}$ on her two qubits A_1, A_2. Next Alice acts $T_2(x,t)$ on A_1A_2 and executes two Hadamard gate transformation $H_{A_1} \otimes H_{A_2}$. Then, she measures her two qubits in the basis $|a_1\rangle_{A_1}\langle a_1| \otimes |a_2\rangle_{A_2}\langle a_2|(a_1, a_2 = 0, 1)$ and sends the results a_1a_2 and x to Bob. As we have mentioned, the transmission of x is to let Bob choose $R_2(x)$ correctly. With these information, Bob's recovery operations are taken as $\left[\mathfrak{r}^{Y_1}(a_1) \otimes \mathfrak{r}^{Y_2}(a_2)\right] R_2(x)$, where $\mathfrak{r}(y) = (1-y)\sigma_0 + y\sigma_3$. Finally, our protocol is completed faithfully and determinedly through the above five steps.

III. CONTROLLED RIO IN THE CASES OF ONE QUBIT USING ONE GHZ STATE

Now, let us first investigate the controlled remote implementations of quantum operations belonging to restricted sets of one qubit using one GHZ states. Without loss of generality, we can write the initial state in a symmetric form of three partite subsystems:

$$\left|\Psi^{\text{ini}}\right\rangle = |\text{GHZ}_+\rangle_{ABC}|\chi\rangle_X|\xi\rangle_Y|\zeta\rangle_Z, \tag{8}$$

where the GHZ state has the form

$$|\text{GHZ}_+\rangle = \frac{1}{\sqrt{2}}\left(|000\rangle + |111\rangle\right). \tag{9}$$

It is shared by Alice, Bob and Charlie. While $|\chi\rangle_X$, $|\xi\rangle_Y$ and $|\zeta\rangle_Z$ are all unknown states of one qubit system. The six qubits of the joint system are divided into three pairs, in which, the qubits A and X belong to Alice, the qubits B and Y belong to Bob, and the qubits C and Z belong to Charlie. Obviously, their roles are initially symmetric for the remote implementations of quantum operations of one qubit.

In order to clearly express our protocol and strictly prove it, specially, for the cases of multiqubits, we denote that the Hilbert space of the joint system is initially taken as a direct product of all qubit Hilbert spaces according to the following sequence:

$$H = H_A \otimes H_B \otimes H_C \otimes H_X \otimes H_Y \otimes H_Z. \tag{10}$$

We can simply call this direct-product "space structure" and denote it by a bit-string, for example, the space structure of the above Hilbert space is $ABCXYZ$. Note that the above space structure is only a notation rule used here, it is absolutely not a precondition of the protocols. If we would like to prove our protocols generally for the cases of multiqubits, such a kind of notation rule is convenient. This fact can be seen in Appendix A. Obviously, since taking such a space structure, the subspaces belonging to Alice, or Bob, or Charlie are separated. This will lead to inconvenience in the whole-space expression of local operations. Therefore, there is the need to change the space structure. This can be realized by a series of swapping transformations, which is studied in Appendix A.

In our protocols, in spite that only local operations and classical communication are used, the problems we deal with are related with the whole system because there is entanglement among various partite subsystems. However, knowing the space structure will be helpful for us to understand the effect of local operations. In fact, our protocol can be found due partially to the reasons that we clearly express an appreciate space structure and general swapping transformations. Therefore, in the following we keep the above sequence of direct products of qubit spaces via the whole-space expressions of our formula in the joint system.

From the symmetric initial state (8), it is easy to find that any one partite subsystem of them plays a possible role among of a sender, a receiver and a controller in the protocols. In other words, when a controller is fixed to a given partite subsystem, thus, the other two partite subsystems play a sender and a receiver, respectively. Under a controller's permission, the remote implementations of quantum operations belonging to the restricted sets is faithfully and determinedly completed between the other two subsystems (locations).

Actually, we are always able to swap their positions in a given space structure among three partite subsystems using so-called general swapping transformations that are studied in Appendix A. Without loss of generality, as soon as a controller is chosen or dominated, we can rewrite the initial state space structure as

$$H_{\text{Controller}} \otimes H_{\text{Sender}} \otimes H_{\text{Receiver}} \otimes H_{\text{Unknown State}}. \tag{11}$$

This means that the first qubit belongs to the controller, the second qubit is in the sender's partite subsystem (the local subsystem), the third qubit is mastered by the receiver, and the fourth qubit is an unknown state in the receiver's hands. Obviously, the unknown states belong to sender and controller are needless in the protocol as soon as the roles of attendees are fixed.

When introducing a controller, our protocol of controlled remote implementations of quantum operations belonging to the restricted sets is made up of seven steps, in which, there are four steps of quantum operations including measurement and three times of classical communications. They are described as the following:

Controlling Step: This step is carried out by the controller. He/She performs a Hadamard transformation

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{12}$$

on his/her controlled qubit $|\gamma\rangle$, and then measures it in the computational basis $|\gamma\rangle\langle\gamma|$ ($\gamma = 0, 1$), that is

$$\mathcal{C}(\gamma) \ = \ (|\gamma\rangle\langle\gamma|H) \otimes I_8, \tag{13}$$

where I_m is a m dimensional identity matrix.

This step is a key matter in our protocol. In fact, when the controller has not done it, there is no quantum entanglement between any two partite subsystems, so there is no any feasible remote implementations of operations. Only if a controller agrees or wishes that the other two partite subsystems implement the RIO protocol, he/she carries out this operation and measurement. Its action is to open the quantum channel between the sender and receiver that is necessary for the remote implementation of operations belonging to the restricted sets in a faithful and determined way.

Allowing Step: This step is still completed by the controller, that is, he/she transfers one c-bit $\boldsymbol{\gamma}$ to the sender or the receiver, which is denoted by $C_{\rm cs}(\gamma)$ or $C_{\rm cr}(\gamma)$, respectively.

This allowing step as well as the above controlling step can be arranged at any time in the RIO process, however, the different arrangement will result in influences on the steps of our protocols. If the classical bit γ is arranged to transfer to the sender, this communication has to be done before the other parts of sending operations. If the classical bit γ is chosen to transfer to the receiver, this communication is able to be done at the beginning (before receiver's preparation), or in the middle (before the recovered operations), or at the end (after the standard recovered operations). At these cases, although the receiver can have the different choices to finish the protocol, we prefer to use a unified method for the RIO of one qubit, that is, we use the classical information γ before the end of our protocol.

This step can be understood figuratively as that the controller distributes the "password" γ to one of the sender and receiver, or gives an authorization to one of them, or says last word (to the receiver) in our protocols. This indicates the role of controller is very important and indispensable. Without the password distribution by the controller, the sender and receiver cannot faithfully and determinedly complete the RIO. This can be clearly seen in the following proofs about our protocols.

Preparing Step: This step is carried out by the receiver. There are two kinds of cases, respectively, based on whether the classical information from the controller is obtained by the receiver or not.

⋄ Case one: If the receiver does not obtain the classical information from the controller, he/she first performs a controlled-NOT using his/her the qubit occupied by the unknown state as a control, his/her shared part (the qubit

$|\beta\rangle$) of the GHZ state as a target, and then measures his/her shared part of the GHZ state in the computational basis $|\beta\rangle\langle\beta|$ ($\beta = 0, 1$), that is

$$\begin{aligned}\mathcal{P}(\beta) &= I_4 \otimes [(|\beta\rangle\langle\beta|) \otimes \sigma_0]\,[\sigma_0 \otimes (|0\rangle\langle 0|) + \sigma_1 \otimes (|1\rangle\langle 1|)] \\ &= I_4 \otimes [(|\beta\rangle\langle\beta|) \otimes \sigma_0]\, C^{\rm not}(2,1),\end{aligned} \tag{14}$$

where σ_0 is 2×2 identity matrix and σ_i ($i = 1, 2, 3$) are the Pauli matrices, and $C^{\rm not}$ is a controlled-NOT defined by

$$C^{\rm not}(2,1) = \sigma_0 \otimes (|0\rangle\langle 0|) + \sigma_1 \otimes (|1\rangle\langle 1|) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}. \tag{15}$$

while $(2, 1)$, as the variable of $C^{\rm not}$, indicates that the second qubit is a control and the first qubit is a target.

The purpose of this step is to let the unknown state be correlated with the sender's local qubit. This is a precondition that the sender is able to remotely implement a quantum operation belonging to the restricted sets.

⋄ Case two: If the controlling step has happened and the receiver gets the classical bit γ from the controller, the preparing step has three different forms according to the time to obtain the classical bit c in general.

(1) When the classical bit γ is known at the beginning of this step, the receiver has to add a prior operation

$$\mathcal{P}^{\rm pre}(\gamma) = I_4 \otimes [(1-\gamma)\sigma_0 + \gamma\sigma_3] \otimes \sigma_0 = I_4 \otimes \mathfrak{r}(\gamma) \otimes \sigma_0 \tag{16}$$

before the above operation (14). Here $\mathfrak{r}(a)$ is a diagonal phase gate with a parameter that is defined by

$$\mathfrak{r}(z) = (1-z)\sigma_0 + z\sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & 1-2z \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & (-1)^z \end{pmatrix}. \tag{17}$$

Note that $z = 0, 1$, and then $(-1)^z = 1 - 2z$. Of course, since it commutes with the project measurement, it also can be inserted between the measurement and the controlled not in the operation (14).

(2) When the classical bit γ is known after the operation (14) or before next recovery operation, the receiver performs a supplementary operation

$$\mathcal{P}^{\rm aft}(\gamma) = I_4 \otimes \mathfrak{r}(\gamma) \otimes \mathfrak{r}(\gamma), \tag{18}$$

where we have used the fact that

$$(\mathfrak{r}(\gamma) \otimes \mathfrak{r}(\gamma)) \left[(|\beta\rangle\langle\beta| \otimes \sigma_0)\, C^{\rm not}(2,1)\right] = \left[(|\beta\rangle\langle\beta| \otimes \sigma_0)\, C^{\rm not}(2,1)\right] (\mathfrak{r}(\gamma) \otimes \sigma_0). \tag{19}$$

(3) When the classical bit γ is known after the next recovery operation, this case is discussed putting in the following recovery step. It is clear that for the above two cases, the receiver always can delay using the classical information up to after recovery operation. Therefore, this case is more general. However, it will be seen that the delaying method is able to lead in the unexpected complication in the recovery step for the cases of multiqubits.

Classical Communication from receiver to the sender: This step is that the receiver transfers a c-bit $\boldsymbol{\beta}$ to the sender, which is denoted by $C_{\rm rs}(\beta)$.

The aim of this step is that the receiver tells the sender that he/she is ready for receiving the remote operation, as well as his/her preparing way.

It must be emphasized that for the cases of one qubit, the receiver's preparing has two equivalent ways with respect to $\beta = 0$ or 1, respectively. If the receiver first fixes the value of β and tells the sender before the beginning of protocol, this step can be saved. In particular, when β is just taken as 0, the sender also does not need the transformation σ_β in the next step, since σ_0 is trivial.

Sending step: This step is carried out by the sender. There are two cases.

⋄ Case one: There is no classical information transferred from the controller to the sender. Thus, after receiving a classical bit β from the receiver, the sender carries out her/his sending operations which are made of four parts (or five parts in the case two). The first one is simple σ_β

$$\mathcal{P}_S(\beta) = I_2 \otimes \sigma_\beta \otimes I_4. \tag{20}$$

The second part of sending step is the operation $U(d, u)$ to be remotely implemented acting on his/her local system (the qubit $|\alpha\rangle$, a shared part of the GHZ state). The third part of sending step is simple a Hadamard gate. The

fourth, also the final part is a measurement on the computational basis $|\alpha\rangle\langle\alpha|$ ($\alpha = 0, 1$). All parts of Alice's sending can be jointly written as

$$\mathcal{S}(\alpha, \beta; d, u) = \{\sigma_0 \otimes (|\alpha\rangle\langle\alpha|) [HU(d, u)\sigma_\beta] \otimes I_4\} . \tag{21}$$

The action of the first part σ_β is to perfectly prepare the state of joint system as such a superposition that the basis in the locally acted system (belonging to sender's subsystem) of every component state is the same as its basis in the remotely operated system (belonging to the space of unknown state in Bob's subsystems) and the corresponding coefficients are just ones of unknown state.

The second part of sending step is just an operation belonging to the restricted sets, which will be remotely implemented in our protocol.

The third part of sending step, the Hadamard gate, is often seen in quantum computation and quantum communication. Its action is similar to the cases in the teleportation of states.

The fourth part of sending step is a measurement on the computational basis whose aim is to project to the needed result.

⋄ Case two: The sender obtains the classical information γ from the controller, he/she has to add to a prior operation

$$\mathcal{S}^{\rm add}(\gamma) = \sigma_0 \otimes [(1-\gamma)\sigma_0 + \gamma\sigma_3] \otimes I_4 = \sigma_0 \otimes \mathfrak{r}(\gamma) \otimes I_4 \tag{22}$$

at the beginning of this step. This means that the sending step becomes

$$\mathcal{S}^{\rm all}(\alpha, \beta, \gamma; d, u) = \{\sigma_0 \otimes (|\alpha\rangle\langle\alpha|) [HU(d, u)\sigma_\beta] \otimes I_4\} \mathcal{S}^{\rm add}_A(\gamma). \tag{23}$$

Classical Communication from sender to receiver: This step is that the sender transfers the classical information α and d to the receiver, which is denoted by $C_{\rm sr}(\alpha; d)$.

This step is that sender tells the receiver what measurement (denoted by α) has been done and which kind of operations (denoted by d) has been transferred. In our protocol, the sender has a one to one mapping table to indicate a kind of restrict set by a value of classical information. For the cases of one qubit, it can be encoded by one c-bit, in which, 0 denotes a restricted set of diagonal operations and 1 denotes a restricted set of antidiagonal operations.

Recovery Step: This step is carried out by the receiver. After receiving a classical bit α from the sender, the receiver first requires to do a recovery operation that consists of two parts or three parts. The first part is $\mathfrak{r}(\alpha)$ and the second part is a fixed form of a restricted set which has the same structure as the $U(d, u)$ to be transferred remotely but its nonzero elements are set as 1. For the cases of one qubit, the fixed forms of the restricted sets of diagonal- and antidiagonal operations are, respectively, σ_0 and σ_1. Therefore, the receiver's recovery operations are written as

$$\mathcal{R}(\alpha; d) = I_8 \otimes [\mathfrak{r}(\alpha)\sigma_d] , \tag{24}$$

where $d = 0$ or 1.

It must be emphasized that the above $\mathcal{R}(\alpha; d)$ only can guarantee the operation $U(d, u)$ is faithfully and determinedly transferred, if the protocol sets that the controller transfers his/her classical bit γ before its action. Just as statement above, if γ is transferred to the sender, the sender has a prior preparation part; when γ is sent to the receiver before the his/her preparing step, he/she can add a supplementary part at the beginning, in the middle or at the end of the preparing step. Obviously, at the end of the preparing is just before the recovering, and so we can move this supplementary part to here. However, if the receiver obtains γ from the controller after the above $\mathcal{R}(\alpha; d)$ action, the receiver has to perform an additional recovery part

$$\mathcal{R}^{\rm aft}(\gamma; d) = (-1)^{\gamma d} I_4 \otimes \mathfrak{r}(\gamma) \otimes \mathfrak{r}(\gamma), \tag{25}$$

where $\mathfrak{r}(z)$ is defined in Eq. (17). Note that $\mathfrak{r}(\gamma)|\beta\rangle\langle\beta| = (-1)^{\gamma\beta}|\beta\rangle\langle\beta|$, we obtain its another form

$$\mathcal{R}^{\rm aft}(\beta, \gamma; d) = (-1)^{\gamma(d+\beta)} I_8 \otimes \mathfrak{r}(\gamma). \tag{26}$$

It is clear that when the protocol sets the controller transfers his/her classical bit γ to the receiver, we always can delay using the classical information γ. In other words, in order to standardize the protocol in the cases of one qubit, we do not add any $\mathcal{P}^{pre}$ and $\mathcal{P}^{aft}$ in the preparing step, but we always use the above $\mathcal{R}^{\rm aft}$ at the end of the protocol. Thus, the whole recovery operations are

$$\mathcal{R}^{\rm all}(\alpha, \gamma, d) = \mathcal{R}^{\rm aft}(\gamma; d)\mathcal{R}(\alpha; d). \tag{27}$$

However, for the case of multiqubits, it is not so simple. Generally, we put the additional recovery operations before the standard recovery operations (24), even before the preparing step in order to have the simplest additional operations for the cases of multiqubits. Of course, if we persist put the additional recovery operation in the last, we will pay a price that it gets a little complication in expressing.

In summary, when there is a controller, we have propose four kinds of protocols for controlled remote implementation of operations belonging to the restricted sets. (1) the sender obtains password; (2)-(4) the receiver obtains password respectively before the preparing, after the preparing (before the recovering) and after the recovering. The second, third and fourth kinds of our protocols can be unitedly expressed without obvious difficulty in the case of one qubit. If the controller transfers his classical bit γ to the sender, the sequence of the above steps in our protocol will become

$$\mathcal{C}(\gamma) \to C_{\rm cs}(\gamma) \to \mathcal{P}(\beta) \to C_{\rm rs}(\beta) \to \mathcal{S}^{\rm all}(\alpha,\beta,\gamma;d) \to C_{\rm sr}(\alpha;d) \to \mathcal{R}(\alpha;d), \tag{28}$$

if the controller transfers his classical bit γ to the receiver, the sequence of the above steps in our protocol is

$$\mathcal{C}(\gamma) \to C_{\rm cr}(\gamma) \to \mathcal{P}(\beta) \to C_{\rm rs}(\beta) \to \mathcal{S}(\alpha,\beta;d) \to C_{\rm sr}(\alpha;d) \to \mathcal{R}^{\rm all}(\alpha,\gamma;d). \tag{29}$$

It is clear that transferring γ to the sender or the receiver can be figuratively understood as distributing a "password", in special, while transferring γ to the receiver at the end of protocol, it can be figuratively understood as "saying last word". They are both important controlled means. Besides the password distributing, the controller owns the right to open the quantum channel. All of this are some main features of a controlled process. Therefore, we called the above process as a controlled remote implementations of operations.

Now, as an example, we fix the controller as Charlie, Alice as a sender and Bob as a receiver without loss of generality. Thus, the initial state is simplified as

$$\left|\Psi^{\rm ini}_{ABCY}\right\rangle = F_4^{-1}(1,3)\left[|{\rm GHZ}_+\rangle_{CAB}|\xi\rangle_Y\right], \tag{30}$$

where $F_3(1,3)$ is a forward rearrangement made of two swapping transformations between the neighbor qubits, which is defined in Appendix A. Similarly, we can discuss the other choices of the controller, sender and receiver, but we do not intend to discuss here.

If we set that the Charlie (controller) transfers the password to sender. It is the first kind of our protocols. All of the operations and measurements in our protocol can be jointedly written as

$$\begin{aligned}\mathcal{I}_R(a,b,c;d) \;=\; & F_4^{-1}(1,3)\left\{\left(|c\rangle_C\langle c|H^C\right)\otimes\left(|a\rangle_A\langle a|H^A U(d,u)\sigma_b^A\mathfrak{r}(c)\right)\right.\\ & \left.\otimes\left[(\sigma_0\otimes\mathfrak{r}(a))\,C^{\rm not}\right]\right\}F_4(1,3).\end{aligned} \tag{31}$$

Note that the operations with the superscripts A, C denote their Hilbert spaces belonging, respectively, to the spaces of qubits A, C. Sometimes, if there is no any confusion, we omit these superscripts. This whole space form of our protocol has covered up the sequence of operations and steps of classical communication, but its advantage is clear. Its action on the initial state (30) yields

$$\left|\Psi^{\rm final}_{ABCY}(a,b,c;d)\right\rangle = \mathcal{I}_R(a,b,c;d)\left|\Psi^{\rm ini}_{ABCY}\right\rangle = \frac{1}{2\sqrt{2}}|abc\rangle_{ABC}\otimes U(d,u)|\xi\rangle_Y. \tag{32}$$

The unknown state to be remotely implemented is just $|\xi\rangle_Y$ in Bob's partite subsystem defined by Eq.(3). Our protocol is then determinedly and faithfully completed.

When setting that Charlie's information transfers to Alice, the whole process of controlled remote implementation of quantum operations belonging to the restricted sets is shown in Fig.2.

Here, we only express the full operations for the first kind of our protocols, and provide its figure of quantum circuit. For the other three kinds of our protocols, the full operations and the figures of quantum circuits are similar. In addition, we should notice that the controller cannot choose who is a sender and who is a receiver in the other two partite subsystems. In other words, when Charlie is a controller, either of Alice and Bob can be chosen as a sender and the other one partite subsystem plays a receiver.

In the end of this section, let us prove our above protocol in detail. For simplicity, we only consider the cases that Alice is a sender, Bob is taken as a receiver, and Charlie is a controller. Initially, the joint system is in the state (30). When Charlie agrees or wishes that Alice and Bob can carry out the remote implementations of quantum operations belonging the restricted sets, he will open the quantum channel between them by preforming the controlling operation

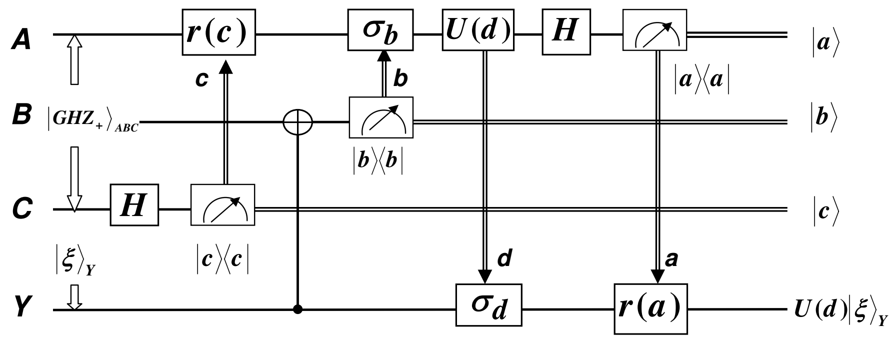

FIG. 2: Quantum circuit of the controlled remote implementations of quantum operations with a controller Charlie. Here, $U(d)$ belonging to the restricted sets is a quantum operation to be remotely implemented, H is a Hadamard transformation, σ_b, σ_d are identity matrices or NOT gates (σ_1) for $b, d = 0$ or $b, d = 1$ respectively, and $r(x) = (1-x)\sigma_0 + x\sigma_3$ is equal an identity matrix if $x = 0$ or a phase gate if $x = 1$. The measurements $|a\rangle\langle a|$,$|b\rangle\langle b|$ and $|c\rangle\langle c|$ are carried out in the computational basis ($a, b, c = 0, 1$). "⇒" (crewel with an arrow) indicates the transmission of classical communication to the location of arrow direction.

on his qubit. His action gives

$$\begin{aligned}\left|\Psi^C_{ABCY}(c)\right\rangle &= F_4^{-1}(1,3)\mathcal{C}(c)F_4(1,3)\left|\Psi^{\rm ini}_{ABCY}\right\rangle \\ &= \frac{1}{2}F_4^{-1}(1,3)\left[|c\rangle_C \otimes (|00\rangle_{AB} + (-1)^c|11\rangle_{AB}) \otimes |\xi\rangle_Y\right] &(33)\\ &= \frac{1}{2}F_4^{-1}(1,3)\left(\sigma_0 \otimes \mathfrak{r}(c) \otimes I_4\right)\left[|c\rangle_C \otimes (|00\rangle_{AB} + |11\rangle_{AB}) \otimes |\xi\rangle_Y\right] &(34)\\ &= \frac{1}{2}F_4^{-1}(1,3)\left(I_4 \otimes \mathfrak{r}(c) \otimes \sigma_0\right)\left[|c\rangle_C \otimes (|00\rangle_{AB} + |11\rangle_{AB}) \otimes |\xi\rangle_Y\right], &(35)\end{aligned}$$

where we have used the definition of $\mathfrak{r}(y)$ in Eq. (17). Thus, Alice and Bob now share a Bell state, and they can carry out the protocol of RIO. However, because HPV protocol is dependent on the type of Bell state, Charlie has to send the "password" c to Alice or Bob. Actually, this indicates the Charlie has his control right.

We need to consider two cases.

The first case is that the protocol sets Charlie to transfer his classical information c to Alice. Using $\mathcal{P}(b)$, Bob prepares his state as

$$\begin{aligned}\left|\Psi^P_{ABCY}(b,c)\right\rangle &= F_4^{-1}(1,3)\mathcal{P}(b)F_4(1,3)\left|\Psi^C_{ABCY}\right\rangle \\ &= \frac{1}{2}\left[F_4^{-1}(1,3)\left(I_2 \otimes \mathfrak{r}(c) \otimes I_4\right)\right]|c\rangle_C \otimes \left\{\sigma_0 \otimes \left[\left(|b\rangle\langle b| \otimes \sigma_0\right)C^{\rm not}\right]\right\} \\ &\quad \times \left[\sum_{k=0}^{1} y_k \left(|00k\rangle_{ABY} + |11k\rangle_{ABY}\right)\right]. &(36)\end{aligned}$$

Note that

$$\begin{aligned}&\left\{\sigma_0 \otimes \left[\left(|b\rangle\langle b|\right)C^{\rm not}(2,1)\right]\right\}\left[\left(|00k\rangle + |11k\rangle\right)\right] \\ =\ &\left[\sigma_0 \otimes \left(|b\rangle\langle b|\right) \otimes \sigma_0\right]\left\{\left(|000\rangle + |110\rangle\right)\delta_{k0} + \left(|011\rangle + |101\rangle\right)\delta_{k1}\right\} \\ =\ &\left(|0b0\rangle\delta_{b0} + |1b0\rangle\delta_{b1}\right)\delta_{k0} + \left(|0b1\rangle\delta_{b1} + |1b1\rangle\delta_{b0}\right)\delta_{k1} \\ =\ &\left[|bb0\rangle\left(\delta_{b0} + \delta_{b1}\right)\delta_{k0} + |(1-b)b1\rangle\left(\delta_{b1} + \delta_{b0}\right)\delta_{k1}\right] \\ =\ &\left(\sigma_b \otimes I_4\right)\left(\delta_{k0}|0b0\rangle + \delta_{k1}|1b1\rangle\right) \\ =\ &\left(\sigma_b \otimes I_4\right)\left(\delta_{k0} + \delta_{k1}\right)|kbk\rangle \\ =\ &\left(\sigma_b \otimes I_4\right)|kbk\rangle, &(37)\end{aligned}$$

where we have used the facts that $\sigma_b|b\rangle = |0\rangle$ and $\sigma_b|1-b\rangle = |1\rangle$ for $b = 0, 1$. It results in

$$\left|\Psi^P_{ABCY}(b,c)\right\rangle = \frac{1}{2}\left[F_4^{-1}(2,4)\left(\mathfrak{r}(c)\sigma_b \otimes I_8\right)\right]\left[\left(y_0|00\rangle_{AY} + y_1|11\rangle_{AY}\right) \otimes |bc\rangle_{BC}\right]. \tag{38}$$

After Bob is ready, he transfers a classical bit b in order to tell Alice his preparing way. So Alice starts with a supplementary operation so that the state of joint system is perfectly ready via the (22), that is

$$\begin{aligned}\left|\Psi_f^P(b,c)\right\rangle &= F_4^{-1}(1,3)\mathcal{S}_A^{\rm add}(c)F_4(1,3)\left|\Psi_{ABCY}^P\right\rangle \\ &= \frac{1}{2}F_4^{-1}(2,4)\left[(\sigma_b\otimes\sigma_0)\left(y_0|00\rangle_{AY}+y_1|11\rangle_{AY}\right)\otimes|b\rangle_B|c\rangle_C\right]. \end{aligned}\tag{39}$$

Therefore, Alice's sending step yields

$$\begin{aligned}\left|\Psi^S(a,b,c;d)\right\rangle &= F_4^{-1}(1,3)\mathcal{S}^{\rm all}(a,b,c,d)F_4(1,3)\left|\Psi_{ABCY}^P\right\rangle \\ &= \frac{1}{2}F_4^{-1}(2,4)\left\{\left[\sum_k^1 y_k\langle a|HU(d,u)|k\rangle|a\rangle_A|k\rangle_Y\right]\otimes|bc\rangle_{BC}\right\}. \end{aligned}\tag{40}$$

The second case is that the protocol sets Charlie to transfer his classical information c to Bob. If Bob choose to first perform $\mathcal{P}^{\rm pre}$, then its action is the same as Alice's. Therefore, when Alice finishes the sending operation, we also obtain Eq. (40). Note that $\mathcal{P}^{\rm aft}(c)\mathcal{P}(b)=\mathcal{P}(b)\mathcal{P}^{\rm pre}(c)$, we can, after $\mathcal{P}(b)$ acting, use $\mathcal{P}^{\rm aft}(c)$. From $\mathcal{R}(a;d)\mathcal{P}^{\rm aft}(c)=(-1)^{cd}\mathcal{P}^{\rm aft}(c)\mathcal{R}(a;d)$, this also means that Bob can delay the additional recovery operation to the end. It is clear that the results of three kinds of procedures are the same.

Now, Bob performs recovery operation (24). From the relation that $U(d,u)=U(0,u)\sigma_d$, and the facts that $U(0,u)=\sum_{j=0}^1 u_j|j\rangle\langle j|$ and $\mathfrak{r}(a)=\sum_{l=0}^1(-1)^{al}|l\rangle\langle l|$, it follows that

$$\begin{aligned}\left|\Psi^{\rm final}(a,b,c;d)\right\rangle &= F_4^{-1}(1,3)\mathcal{R}(a,d)F_4(1,3)\left|\Psi_{ABCY}^S\right\rangle \\ &= \frac{1}{2}F_4^{-1}(2,4)\left\{\left[\sum_k^1 y_k\langle a|HU(d,u)|k\rangle|a\rangle_A\left(\mathfrak{r}(a)\sigma_d|k\rangle_Y\right)\right]\otimes|bc\rangle_{BC}\right\} \\ &= \frac{1}{2}|a\rangle_A\otimes F_3^{-1}(1,3)\left\{\left[\sum_{j=0}^1\sum_{k=0}^1\sum_{l=0}^1 u_jy_k\langle a|H|j\rangle\right.\right. \\ &\quad \left.\left.\times\left(\langle j|\sigma_d|k\rangle(-1)^{al}\langle l|\sigma_d|k\rangle\right)|l\rangle_Y\right]|bc\rangle_{BC}\right\}. \end{aligned}\tag{41}$$

Note that

$$\langle j|\sigma_d|k\rangle\langle l|\sigma_d|k\rangle=\langle j|\sigma_d|k\rangle\delta_{jl},\tag{42}$$

we have

$$\left|\Psi^{\rm final}(a,b,c;d)\right\rangle = \frac{1}{2}|a\rangle_A\otimes F_3^{-1}(1,3)\left\{\left[\sum_{j=0}^1\sum_{k=0}^1 u_jy_k(-1)^{aj}\langle a|H|j\rangle\langle j|\sigma_d|k\rangle|j\rangle_Y\right]\otimes|bc\rangle_{BC}\right\}.\tag{43}$$

Since

$$(-1)^{aj}\langle a|H|j\rangle=\frac{1}{\sqrt{2}}\tag{44}$$

for any a and j, the above equation becomes

$$\begin{aligned}\left|\Psi^{\rm final}(a,b,c;d)\right\rangle &= \frac{1}{2\sqrt{2}}|a\rangle_A\otimes F_3^{-1}(1,3)\left\{\left[\sum_{j=0}^1\sum_{k=0}^1 u_jy_k\langle j|\sigma_d|k\rangle|j\rangle_Y\right]\otimes|bc\rangle_{BC}\right\} \\ &= \frac{1}{2\sqrt{2}}|a\rangle_A\otimes F_3^{-1}(1,3)\left\{\left[\sum_{k=0}^1 y_kU(0,u)\sigma_d|k\rangle_Y\right]\otimes|bc\rangle_{BC}\right\} \\ &= \frac{1}{2\sqrt{2}}|abc\rangle_{ABC}\otimes U(d,u)|\xi\rangle_Y. \end{aligned}\tag{45}$$

That is, we obtain the conclusion (32) of our protocol. Therefore, we finish the proof our protocols of controlled RIO with a controller in the cases of one qubit.

IV. COMBINED RIO IN THE CASE OF ONE QUBIT USING ONE GHZ STATE

Now, let us consider a quantum operation that is a product of two parts $\mathcal{U}_2$ and $\mathcal{U}_1$, that is, $\mathcal{U}=\mathcal{U}_2\mathcal{U}_1$. Assuming $\mathcal{U}_1$ and $\mathcal{U}_2$ both belong to the restricted sets, we can denote them by $U(d_1,u)$ and $U(d_2,v)$, respectively, in our notation. Thus, the remote implementation of $\mathcal{U}$ can be completed via sending $\mathcal{U}_1$ and $\mathcal{U}_2$ in turn by one sender in the known protocols [3, 4], but two shared Bell pairs are needed. However, we find that this task can be faithfully and determinedly completed by two senders via one GHZ state. Moreover, we will see that the RIO protocol with two senders using one GHZ state has higher security compared with one using two Bell states. More analysis about the security enhancement has been given in our introduction.

Without loss of generality, we set Alice and Bob as two senders, and Alice first sends $U(d_1,u)$, Bob then sends $U(d_2,v)$. Charlie plays a receiver. Except for the unknown state is replaced by $|\zeta\rangle=z_0|0\rangle_Z+z_1|1\rangle_Z$, the initial state has not the other difference form Eq. (30). Since the significance and actions of the most related operations have been explained in Sec. III, we do not intend to repeat them here. Our protocol is made of the following seven steps.

Step one: Charlie's preparing.

$$\mathcal{P}_C(c)=I_4\otimes\left[\left(|c\rangle_C\langle c|\right)\otimes\sigma_0^Z\right]\left[\sigma_0^C\otimes\left(|0\rangle_Z\langle 0|\right)+\sigma_1^C\otimes\left(|1\rangle_Z\langle 1|\right)\right]. \tag{46}$$

Step two: First classical communication. Charlie sends the classical information c to Alice and Bob.

Step three: Alice's sending.

$$\mathcal{S}_A(a,c;d_1,u)=\left(|a\rangle_A\langle a|\right)\left[H^AU(d_1,u)\right]\sigma_c^A\otimes I_8. \tag{47}$$

Step four: Second classical communication. Alice sends the classical information d_1 to Bob and a to Charlie.

Step five: Bob's sending.

$$\mathcal{S}_B(b,c;d_1,d_2,v)=\sigma_0\otimes\left(|b\rangle_B\langle b|\right)\left[H^BU(d_2,v)\right]\left(\sigma_{d_1}^B\sigma_c^B\right)\otimes I_4. \tag{48}$$

Step six: Third classical communication. Bob sends the classical information b and d_2 to Charlie.

Step seven: Charlie's recovering

$$\mathcal{R}_C(a,b;d_1,d_2)=I_4\otimes\sigma_0^C\otimes\left(\mathfrak{r}(b)\sigma_{d_2}\right).\left(\mathfrak{r}(a)\sigma_{d_1}\right). \tag{49}$$

All of the operations and measurements in our above protocol can be jointly written as

$$\begin{aligned}\mathcal{I}_R(a,b,c;d_1,d_2,u,v) &= \left(|a\rangle_A\langle a|H^AU(d_1,u)\sigma_c^A\right)\otimes\left(|b\rangle_B\langle b|H^BU(d_2,v)\sigma_{d_1}\sigma_c^A\right)\\ &\quad\times\left[\left(|c\rangle\langle c|\otimes\mathfrak{r}(b)\sigma_{d_2}\mathfrak{r}(a)\sigma_{d_1}\right)C^{\mathrm{not}}\right].\end{aligned} \tag{50}$$

Its acting on the initial state gives

$$\left|\Psi_C^{\mathrm{final}}(a,b,c;d_1,d_2,u,v)\right\rangle=\mathcal{I}_R(a,b,c;d_1,d_2,u,v)\left|\Psi_C^{\mathrm{ini}}\right\rangle=\frac{1}{2\sqrt{2}}|abc\rangle_{ABC}\otimes U(d_2,v)U(d_1,u)|\zeta\rangle_Z, \tag{51}$$

where $a,b,c=0,1$ denote the spin up or down, and $d_1,d_2=0$ and $d_1,d_2=1$ respectively indicate the operations of diagonal and antidiagonal restricted sets. Therefore, the remote implementations of the combination of two quantum operations belonging to restricted sets are faithfully and determinedly completed. It can be called the combined remote implementation of quantum operations which can be displayed by Fig.3.

In order to prove our protocol with two senders, we first need the equation

$$\left\{\sigma_0\otimes\left[\left(|c\rangle\langle c|\otimes\sigma_0\right)C^{\mathrm{not}}(2,1)\right]\right\}|\mathrm{GHZ}_+\rangle\otimes|k\rangle=F_4^{-1}(3,4)\left(\sigma_c\otimes\sigma_c\otimes I_4\right)\left(|kkk\rangle\otimes|c\rangle\right). \tag{52}$$

Its proof is similar to Eq. (37). Therefore, Charlie's preparation gives

$$\begin{aligned}\left|\Psi^P(c)\right\rangle &= \mathcal{P}_C(c)\left|\Psi_{ABCZ}^{\mathrm{ini}}\right\rangle\\ &= \frac{1}{\sqrt{2}}F_4^{-1}(3,4)\left[\left(\sigma_c\otimes\sigma_c\otimes I_4\right)\left(z_0|00\rangle_{AB}\otimes|0\rangle_Y+z_1|11\rangle_{AB}\otimes|1\rangle_Y\right)\otimes|c\rangle_C\right],\end{aligned} \tag{53}$$

where $F_N(i,j)$ is defined in Appendix A.

After receiving the classical information c from Charlie (receiver), Alice supplements a σ_c transformation, and then performs the first sending operations, we have

$$\begin{aligned}\left|\Psi_1^S(a,c;d_1,u)\right\rangle &= \mathcal{S}_A(a,c,d_1,u)\left|\Psi^P(c)\right\rangle\\ &= \frac{1}{\sqrt{2}}F_4^{-1}(3,4)\left[\sum_{k=0}^{1}z_k\left(|a\rangle_A\langle a|HU(d_1,u)|k\rangle\right)\left(\sigma_c|k\rangle_B\right)|k\rangle_Y\right]\otimes|c\rangle_C.\end{aligned} \tag{54}$$

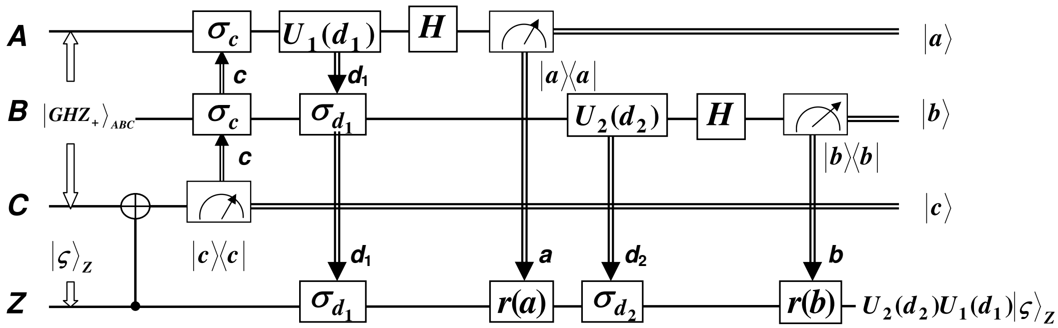

FIG. 3: Quantum circuit of the combined remote implementation of quantum operation with two sender Alice and Bob . Here, $U_1(d_1)$ and $U_2(d_2)$ are respectively a part of the quantum operation $U(d_1,d_2)=U_2(d_2)U_1(d_1)$ that is remotely implemented by combining Alice and Bob's actions, H is a Hadamard transformation, $\sigma_c,\sigma_{d_1},\sigma_{d_2}$ are identity matrices or NOT gates (σ_1) for $c,d_1,d_2=0$ or $c,d_1,d_2=1$ respectively, and $r(x)=(1-x)\sigma_0+x\sigma_3$ is an identity matrix if $x=0$ or a phase gate (σ_3) if $x=1$. The measurements $|a\rangle\langle a|$,$|b\rangle\langle b|$ and $|c\rangle\langle c|$ are carried out in the computational basis ($a,b,c=0,1$). "⇒" (crewel with an arrow) indicates the transmission of classical communication to the location of arrow direction.

Alice again tells Bob d_1 and Charlie a. In succession, based on the classical information c (coming from Charlie) and d_1 (coming from Alice), Bob first carries out $\sigma_{d_1}\sigma_c$, and then performs the second sending operations:

$$\begin{aligned}\left|\Psi_2^S(a,b,c;d_1,d_2,u,v)\right\rangle &= \mathcal{S}_B(b,c,d_2,v)\left|\Psi_1^S(a,c,d_1,u\right\rangle \\ &= \frac{1}{\sqrt{2}}F_4^{-1}(3,4)\left[\sum_{k=0}^{1} z_k\left(|a\rangle_A\langle a|HU(d_1,u)|k\rangle_A\right)\right. \\ &\quad \otimes\left(|b\rangle_B\langle b|HU(d_2,v)\sigma_{d_1}|k\rangle_B\right)|k\rangle_Y\Big]\otimes|c\rangle_C. \end{aligned}\tag{55}$$

Finally, Bob's recovery operation gives

$$\begin{aligned}\left|\Psi^{\rm final}(a,b,c;d_1,d_2,u,v)\right\rangle &= \mathcal{R}_B(a,b,d_1,d_2)\left|\Psi_2^S(a,b,c,d_1,d_2,u,v\right\rangle \\ &= \frac{1}{\sqrt{2}}F_4^{-1}(3,4)\left[\sum_{k=0}^{1} z_k\left(|a\rangle_A\langle a|HU(d_1,u)|k\rangle\right)\right. \\ &\quad \times\left(|b\rangle_B\langle b|HU(d_2,v)\sigma_{d_1}|k\rangle\right) \\ &\quad \otimes\mathfrak{r}(b)\sigma_{d_2}\mathfrak{r}(a)\sigma_{d_1}|k\rangle_Z\Big]\otimes|c\rangle_C. \end{aligned}\tag{56}$$

The remaining steps of this proof is similar to the ones in the end of Sec. III, but it needs to repeat three times. First, using $U(d_1,u)=U(0,u)\sigma_{d_1}=\sum_{j=0}^{1}u_j|j\rangle\langle j|\sigma_{d_1}$ and $\mathfrak{r}(a)=\sum_{l=0}^{1}(-1)^{al}|l\rangle\langle l|$ we have

$$\begin{aligned}\left|\Psi^{\rm final}(a,b,c;d_1,d_2,u,v)\right\rangle &= \frac{1}{\sqrt{2}}\left[\sum_{j=0}^{1}\sum_{k=0}^{1}\sum_{l=0}^{1} u_j y_k\left(|a\rangle_A\langle a|H|j\rangle\langle j|\sigma_{d_1}|k\rangle\right)\right. \\ &\quad \otimes\left(|b\rangle_B\langle b|HU(d_2,v)\sigma_{d_1}|k\rangle\right) \\ &\quad \otimes\mathfrak{r}(b)\sigma_{d_2}(-1)^{al}|l\rangle_Y\langle l|\sigma_{d_1}|k\rangle\Big]\otimes|c\rangle_C. \end{aligned}\tag{57}$$

Because that $\langle j|\sigma_y|k\rangle\langle l|\sigma_{d_1}|k\rangle=\delta_{jl}\langle j|\sigma_y|k\rangle$, it becomes

$$\begin{aligned}\left|\Psi^{\rm final}(a,b,c;d_1,d_2,u,v)\right\rangle &= \frac{1}{\sqrt{2}}|ab\rangle_{AB}\otimes\left[\sum_{j=0}^{1}\sum_{k=0}^{1} u_j y_k\left(\langle a|H|j\rangle(-1)^{aj}\right)\right. \\ &\quad \times\left(\langle b|HU(d_2,v)\sigma_{d_1}|k\rangle\right)\mathfrak{r}(b)\sigma_{d_2}|j\rangle_Y\langle j|\sigma_{d_1}|k\rangle\Big]\otimes|c\rangle_C. \end{aligned}\tag{58}$$

While from $\langle a|H|j\rangle(-1)^{aj}=1/\sqrt{2}$, it follows that

$$\begin{aligned}\left|\Psi^{\rm final}(a,b,c;d_1,d_2,u,v)\right\rangle &= \frac{1}{2}|ab\rangle_{AB}\otimes\left[\sum_{j=0}^{1}\sum_{k=0}^{1} u_j y_k\left(\langle b|HU(d_2,v)\sigma_{d_1}|k\rangle\right)\right. \\ &\quad \times\mathfrak{r}(b)\sigma_{d_2}|j\rangle_Y\langle j|\sigma_{d_1}|k\rangle\Big]\otimes|c\rangle_C. \end{aligned}\tag{59}$$

Again inserted the complete relation after $U(d_2)$ and based on the above same reason, the above equation is reduced to

$$\begin{aligned}\left|\Psi^{\rm final}(a,b,c;d_1,d_2,u,v)\right\rangle &= \frac{1}{2}|ab\rangle_{AB}\otimes\left[\sum_{j=0}^{1}\sum_{k=0}^{1}\sum_{l=0}^{1}u_j y_k\left(\langle b|HU(d_2,v)|l\rangle\langle l|\sigma_{d_1}|k\rangle\right)\right.\\ &\quad\left.\times\mathfrak{r}(b)\sigma_{d_2}|j\rangle_Y\langle j|\sigma_{d_1}|k\rangle\right]\otimes|c\rangle_C\\ &= \frac{1}{2}|ab\rangle_{AB}\otimes\left[\sum_{j=0}^{1}\sum_{k=0}^{1}u_j y_k\left(\langle b|HU(d_2,v)|j\rangle\right)\right.\\ &\quad\left.\times\mathfrak{r}(b)\sigma_{d_2}|j\rangle_Y\langle j|\sigma_{d_1}|k\rangle\right]\otimes|c\rangle_C.\end{aligned}\tag{60}$$

Repeatedly using the above skills, that is $U(d_2)=U(0,v)\sigma_{d_2}=\sum_{i=0}^{1}v_i|i\rangle\langle i|\sigma_{d_2}$ and $\mathfrak{r}(b)=\sum_{l=0}^{1}(-1)^{bl}|l\rangle\langle l|$, we obtain

$$\begin{aligned}\left|\Psi^{\rm final}(a,b,c;d_1,d_2,u,v)\right\rangle &= \frac{1}{2}|ab\rangle_{AB}\otimes\left[\sum_{i=0}^{1}\sum_{j=0}^{1}\sum_{k=0}^{1}\sum_{l=0}^{1}v_i u_j y_k\left(\langle b|H|i\rangle\langle i|\sigma_{d_2}|j\rangle\right)\right.\\ &\quad\left.\times(-1)^{bl}|l\rangle_Y\langle l|\sigma_{d_2}|j\rangle\langle j|\sigma_{d_1}|k\rangle\right]\otimes|c\rangle_C\\ &= \frac{1}{2}|ab\rangle_{AB}\otimes\left[\sum_{i=0}^{1}\sum_{j=0}^{1}\sum_{k=0}^{1}v_i u_j y_k\left(\langle b|H|i\rangle(-1)^{bi}\right)\right.\\ &\quad\left.\times\langle i|\sigma_{d_2}|j\rangle\langle j|\sigma_{d_1}|k\rangle|i\rangle_Y\right]\otimes|c\rangle_C\\ &= \frac{1}{2\sqrt{2}}|ab\rangle_{AB}\otimes\left[\sum_{i=0}^{1}\sum_{j=0}^{1}\sum_{k=0}^{1}v_i u_j y_k\langle i|\sigma_{d_2}|j\rangle\langle j|\sigma_{d_1}|k\rangle|i\rangle_Y\right]\otimes|c\rangle_C\\ &= \frac{1}{2\sqrt{2}}|ab\rangle_{AB}\otimes\left[U(d_2,v)U(d_1,u)|\xi\rangle_Y\right]\otimes|c\rangle_C.\end{aligned}\tag{61}$$

The proof of our protocol with two senders using one GHZ state is finished.

V. PROTOCOLS IN THE CASES OF N QUBITS

We have proposed and proved the protocols of controlled and combined remote implementations of quantum operations for one qubit using one GHZ state, respectively. The controlled RIO has a controller, a sender and a receiver, and the roles of three partite subsystems can be exchanged with each other. The combined RIO has two senders and a receiver, and every sender transfers an operation (or a part of one decomposable operation), two transferred operations are combined together according to the sequence of transferred time to form a total operation that is remotely implemented. In the following let us investigate the cases of multiqubits.

We have seen that since a controller or an extra sender being fetched in the protocols for the cases of one qubit, the entanglement resource really used to the remote implementations of operations is still one Bell pair, in spite that our protocols is carried out via one GHZ state. In other words, the design of adding controller or extra sender will use a part of the entanglement resource. Therefore, for the cases of more than one qubit, our restricted sets [4] are still suitable to our controlled and combined RIOs.

A. Some notations

Usually, in order to avoid the possible errors, we need to denote the sequential structure of direct product space of qubits, or a sequence of direct products of qubit space basis vectors in the multiqubit systems. For Alice's space, we set its sequential structure as $A_1A_2\cdots A_N$, in other words, its basis vector has the form $|a_1\rangle_{A_1}|a_2\rangle_{A_2}\cdots|a_N\rangle_{A_N}$ (or $|a_1a_2\cdots a_N\rangle_{A_1A_2\cdots A_N}$). Similarly, we set the sequential structure of Bob's space as $B_1B_2\cdots B_NY_1Y_2\cdots Y_N$, in other words, its basis vector has the form $|b_1\rangle_{B_1}|b_2\rangle_{B_2}\cdots|b_N\rangle_{B_N}|k_1\rangle_{Y_1}|k_2\rangle_{Y_2}\cdots|k_N\rangle_{Y_N}$. It is clear that for a N-qubit system, its space structure can be represented by a bit-string with the length of N.

In order to write our formula compactly and clearly, and then prove our protocols more conveniently, we need to use some general swapping transformations, for example, $F_N(i,j)$, $P_N(j,k)$, $\Lambda(2,N)$, $\Omega(2,N)$, $\Omega(3,N)$ and $\Upsilon(3,N)$, that are studied in Appendix A and we will not repeatedly write their definitions here.

In addition, we still need to define

$$\Theta_N = \Omega(3,N)\Upsilon^{-1}(3,N) \tag{62}$$

and then introduce

$$\Theta_A(n) = \left(I_{2^n} \otimes \Lambda(2,N) \otimes I_{2^N}\right)\left(\Theta_n \otimes I_{2^{3N-2n)}}\right), \tag{63}$$

$$\Theta_B(n) = \left(I_{2^n} \otimes \Upsilon(3,N)\right)\left(\Theta_n \otimes I_{2^{3N-2n)}}\right), \tag{64}$$

$$\Theta_C(n) = \left(\Theta_n \otimes I_{2^{3N-2n)}}\right). \tag{65}$$

Thus, we have

$$\begin{aligned}
&\Theta_A(n)\left[\left(\bigotimes_{m=1}^{n}|a_m b_m c_m\rangle_{A_m B_m C_m}\right)\left(\bigotimes_{s=n+1}^{N}|a_s b_s\rangle_{A_s B_s}\right)\otimes\left(\bigotimes_{t=1}^{N}|k_t\rangle_{Y_t}\right)\right]\\
&=\left(\bigotimes_{m=1}^{n}|c_m\rangle_{C_m}\right)\left(\bigotimes_{s=n+1}^{N}|a_s\rangle_{A_s}\right)\left(\bigotimes_{m=1}^{N}|b_m\rangle_{B_m}\right)\otimes\left(\bigotimes_{m=1}^{N}|k_m\rangle_{Y_m}\right),
\end{aligned} \tag{66}$$

$$\begin{aligned}
&\Theta_B(n)\left[\left(\bigotimes_{m=1}^{n}|a_m b_m c_m\rangle_{A_m B_m C_m}\right)\left(\bigotimes_{s=n+1}^{N}|a_s b_s\rangle_{A_s B_s}\right)\otimes\left(\bigotimes_{s=1}^{N}|k_s\rangle_{Y_s}\right)\right]\\
&=\left(\bigotimes_{m=1}^{n}|c_m\rangle_{C_m}\right)\left(\bigotimes_{s=1}^{N}|a_s b_s k_s\rangle_{A_s B_s Y_s}\right),
\end{aligned} \tag{67}$$

$$\begin{aligned}
&\Theta_C(n)\left[\left(\bigotimes_{m=1}^{n}|a_m b_m c_m\rangle_{A_m B_m C_m}\right)\left(\bigotimes_{s=n+1}^{N}|a_s b_s\rangle_{A_s B_s}\right)\otimes\left(\bigotimes_{t=1}^{N}|k_t\rangle_{Y_t}\right)\right]\\
&=\left(\bigotimes_{m=1}^{n}|c_m\rangle_{C_m}\right)\left(\bigotimes_{s=1}^{N}|a_s b_s\rangle_{A_s B_s}\right)\otimes\left(\bigotimes_{t=1}^{N}|k_t\rangle_{Y_t}\right).
\end{aligned} \tag{68}$$

Similarly, we can obtain the transformed relations acting on the operations (or matrices).

By comparing with the cases of one qubit, we can extend the controlled and combined RIO protocols to the cases of N qubits in terms of our restricted sets. However, we find that the variety of protocols is more obvious, the expressions and proofs of protocols get a little complicated. Our protocols are still made up of seven steps for controlled and combined remote implementations of N-qubit quantum operations belonging to our restricted sets. For the cases with $n < N$ controllers, we only need n GHZ states and $N-n$ Bell pairs. While when two senders are fetched in, we need N GHZ states.

Without loss of generality, when with n controllers, we set the former n shared entangled states as GHZ states, the initial state reads

$$\left|\Psi_N^{\rm ini}\right\rangle = \left(\bigotimes_{m=1}^{n}|{\rm GHZ}^+\rangle_{A_m B_m C_m}\right)\otimes\left(\bigotimes_{s=n+1}^{N}|\Phi^+\rangle_{A_s B_s}\right)\otimes|\xi\rangle_{Y_1 Y_2\cdots Y_N}, \tag{69}$$

when with two senders, we take the N shared GHZ states, the initial state becomes

$$\left|\Psi_N^{\rm ini}\right\rangle = \left(\bigotimes_{m=1}^{N}|{\rm GHZ}^+\rangle_{A_m B_m C_m}\right)\otimes|\xi\rangle_{Y_1 Y_2\cdots Y_N}, \tag{70}$$

where $|\xi\rangle_{y_1Y_2\cdots y_N}$ is an arbitrary (unknown) pure state in the N-qubit systems:

$$|\xi\rangle_{Y_1\cdots Y_N} = \sum_{k_1,\cdots,k_N=0}^{1} y_{k_1\cdots k_N}|k_1k_2\cdots k_N\rangle. \tag{71}$$

Therefore, we know that the space structures are initially

$$\prod_{m=1}^{n} A_mB_mC_m \prod_{s=n+1}^{N} A_sB_s \prod_{t=1}^{N} Y_t \tag{72}$$

for the case with n controllers, and

$$\prod_{m=1}^{N} A_mB_mC_m \prod_{t=1}^{N} Y_t \tag{73}$$

for the case with two senders.

For simplicity, in the following, we only present the operations and measurements done by the three partite subsystems and omit the steps of classical communications. Of course, we still have to remember the implementing sequence of them. Moreover, we do not detailedly account for the significance and action of every step, which can be understood from the cases of one qubit.

B. With n controllers

For the cases with n controllers, we set Charlies as controllers, Alice as a sender and Bob as a receiver.

The controllers's (Charlies') startup is

$$\mathcal{C}(c_1,\cdots,c_n) = \Theta_C^{-1}(n)\left[\bigotimes_{m=1}^{n}\left(|c_m\rangle_{C_m}\langle c_m|H^{C_m}\right)\otimes I_{2^{3N}}\right]\Theta_C(n). \tag{74}$$

Bob's prior preparation is

$$\mathcal{P}_B^{\rm add}(c_1,c_2,\cdots,c_n) \;=\; \Theta_B^{-1}(n)\left\{I_{2^n}\otimes\left(\bigotimes_{m=1}^{n}\sigma_0^{A_m}\otimes\mathfrak{r}^{B_m}(c_m)\otimes\sigma_0^{Y_m}\right)\otimes I_{2^{3(N-n)}}\right\}\Theta_B(n). \tag{75}$$

Bob's preparing is

$$\begin{aligned}\mathcal{P}_B(b_1,b_2,\cdots,b_N) \;=\; \Theta_B^{-1}(n)\Bigg\{I_{2^n}\otimes\Bigg[\bigotimes_{m=1}^{N}\sigma_0^{A_m}\otimes\left(|b_m\rangle_{B_m}\langle b_m|\otimes\sigma_0^{Y_m}\right)\\ \times\left(\sigma_0^{B_m}\otimes|0\rangle_{Y_m}\langle 0|+\sigma_1^{B_m}\otimes|1\rangle_{Y_m}\langle 1|\right)\Bigg]\Bigg\}\Theta_B(n).\end{aligned} \tag{76}$$

Alice's prior sending is

$$\mathcal{S}_A^{\rm add}(c_1,c_2,\cdots,c_n) \;=\; \Theta_A^{-1}(n)\left\{I_{2^n}\otimes\left(\bigotimes_{m=1}^{n}\mathfrak{r}(c_m)\right)\otimes I_{2^{N-n}}\otimes I_{4^N}\right\}\Theta_A(n). \tag{77}$$

Alice's sending is

$$\begin{aligned}\mathcal{S}_A(a_1,b_1,a_2,b_2,\cdots,a_N,b_N;x,u) \;=\; \Theta_A^{-1}(n)\Bigg\{I_{2^n}\otimes\Bigg[\left(\bigotimes_{m=1}^{N}|a_m\rangle_{A_m}\langle a_m|\right)\left(\bigotimes_{m=1}^{N}H^{A_m}\right)\\ \times T_N^r(x,u)\left(\bigotimes_{m=1}^{N}\sigma_{b_m}^{A_m}\right)\Bigg]\otimes I_{4^N}\Bigg\}\Theta_A(n).\end{aligned} \tag{78}$$

Bob's supplementary recovering is

$$\mathcal{R}_B^{\rm add}(c_1, c_2\cdots c_n) = \left(\bigotimes_{m=1}^{n} \sigma_0^{A_m}\otimes \mathfrak{r}(c_m)\otimes \sigma_0^{C_m}\right)\otimes I_{2^{2(N-n)}}\otimes\left(\bigotimes_{m=1}^{n}\mathfrak{r}(c_m)^{Y_m}\right)\otimes I_{2^{N-n}}. \tag{79}$$

Bob's recovering is

$$\mathcal{R}_B(a_1, a_2\cdots a_N; x) = I_{2^{(2N+n)}}\otimes\left(\bigotimes_{m=1}^{N}\mathfrak{r}(a_m)^{Y_m}\right)R_N(x). \tag{80}$$

In particular, since $R_N(x)\left[\left(\bigotimes_{m=1}^{n}\mathfrak{r}(c_m)^{Y_m}\right)\otimes I_{2^{N-n}}\right]R_N^\dagger(x)$ and $\left(\bigotimes_{m=1}^{N}\mathfrak{r}(a_m)^{Y_m}\right)$ are diagonal, they commute each other. Again from $R_N^\dagger(x)R_N(x)=I_{2^N}$, it follows that

$$\begin{aligned}
&R_N(x)\left[\left(\bigotimes_{m=1}^{n}\mathfrak{r}(c_m)^{Y_m}\right)\otimes I_{2^{N-n}}\right]R_N^\dagger(x)\left[\left(\bigotimes_{m=1}^{N}\mathfrak{r}(a_m)^{Y_m}\right)R_N(x)\right]\\
&=\left[\left(\bigotimes_{m=1}^{N}\mathfrak{r}(a_m)^{Y_m}\right)R_N(x)\right]\left[\left(\bigotimes_{m=1}^{n}\mathfrak{r}(c_m)^{Y_m}\right)\otimes I_{2^{N-n}}\right].
\end{aligned} \tag{81}$$

Therefore, we obtain a final recovery operation

$$\begin{aligned}
\mathcal{R}_B^{\rm aft}(c_1, c_2\cdots c_n; x) \;=\; &\left(\bigotimes_{m=1}^{n} \sigma_0^{A_m}\otimes \mathfrak{r}(c_m)\otimes \sigma_0^{C_m}\right)\otimes I_{2^{2(N-n)}}\\
&\otimes\left\{R_N(x)\left[\left(\bigotimes_{m=1}^{n}\mathfrak{r}(c_m)^{Y_m}\right)\otimes I_{2^{N-n}}\right]R_N^\dagger(x)\right\}.
\end{aligned} \tag{82}$$

Obviously, such a finally additional recovery-operation is complicated in form compared with the other additional operations. Perhaps, it is not worth being used in our protocols.

It must be pointed out that three times of classical communication are, respectively: (1) Charlies to Alice or Bob n c-bits; (2) Bob to Alice N c-bits; (3) Alice to Bob $N+\left[\log_2(2^N!)\right]+1$ c-bits. (x may be encoded by $\left[\log_2(2^N!)\right]+1$ c-bit string, where $[\cdots]$ means taking the integer part).

Based on the kinds and time of the controllers distributing to the sender or receiver, we only can use one beforehand operation for Bob or Alice or Charlies, which has been seen in the cases of one qubit. The whole operations and measurements can be jointly written according to four cases (omitting arguments for simplicity):

(1) Alice (sender) obtains password before her sending

$$\mathcal{I}_R(1)=\mathcal{R}_B\mathcal{S}_A\mathcal{S}_A^{\rm add}\mathcal{P}_B; \tag{83}$$

(2) Bob (receiver) obtains password before his preparation

$$\mathcal{I}_R(2)=\mathcal{R}_B\mathcal{S}_A\mathcal{P}_B\mathcal{P}_B^{\rm add}; \tag{84}$$

(3) Bob (receiver) obtains password after his preparation

$$\mathcal{I}_R(3)=\mathcal{R}_B\mathcal{R}_B^{\rm add}\mathcal{S}_A\mathcal{P}_B; \tag{85}$$

(4) Bob (receiver) obtains password after his recovery operations

$$\mathcal{I}_R(4)=\mathcal{R}^{\rm aft}\mathcal{R}_B\mathcal{S}_A\mathcal{P}_B. \tag{86}$$

C. With two senders

In the case of two senders, we set Bob as a receiver, Alice as the first sender and Charlie as the second sender. It is different from the cases of one qubit, where Charlie is a receiver, Alice is the first sender and Bob is the second sender. However, it is unimportant since the symmetry among three partite subsystems.

Bob's preparation and Alice's sending are the same as the above (76) and (78), but $n = N$. Charlie's second sending is

$$\mathcal{S}_C(c_1, c_2, \cdots, c_N; x, y, v) = \Theta_C^{-1}(N)\left\{\left[\left(\bigotimes_{m=1}^{N} |c_m\rangle_{C_m}\langle c_m|\right)\left(\bigotimes_{m=1}^{N} H^{C_m}\right)\right.\right. \\ \left.\left. \times T_N^r(y,v) R_N(x)\right] \otimes I_{2^{3N}}\right\}\Theta_C(N). \tag{87}$$

Bob's recovery operation is

$$\mathcal{R}_B(a_1, a_2, \cdots, a_N, b_1, b_2, \cdots, b_n, c_1, c_2, \cdots, c_N; x, y) \\ = I_{2^{3N}} \otimes \left[\left(\bigotimes_{m=1}^{N} \mathfrak{r}^{Y_m}(c_m)\right) R_N(y)\right]\left[\bigotimes_{m=1}^{N} \left(\mathfrak{r}^{Y_m}(a_m)\right) R_N(x)\right]\left(\bigotimes_{m=1}^{N} \sigma_{b_m}^{Y_m}\right), \tag{88}$$

where $\mathfrak{r}(y)$ is defined by Eq. (17).

It must be pointed out that four times of classical communication are respectively: (1) Bob to Alice N c-bits and to Charlies N c-bits; (2) Alice to Bob $N + \left[\log_2(2^N!)\right] + 1$ c-bits; (3) Alice to Charlie $\left[\log_2(2^N!)\right] + 1$ c-bits; (4) Charlie to Bob $N + \left[\log_2(2^N!)\right] + 1$ c-bits.

Obviously, the whole operations and measurements can be jointly written as

$$\mathcal{I}_R = \mathcal{R}_B\mathcal{S}_C\mathcal{S}_A\mathcal{P}_B. \tag{89}$$

It is not difficult to prove our protocols for the cases of N qubits because all of steps are similar to the cases of one qubit, which is put in Appendix B.

VI. DISCUSSION AND CONCLUSION

We have investigated the controlled and combined remote implementation of the quantum operations belonging to our restricted sets [4] using GHZ state(s). The main motivations to use GHZ state(s) in our protocols are to enhance security, increase variety, extend applications as well as advance efficiency via fetching in many controllers and two senders.

It must be emphasized that knowing the forms of the restricted sets of quantum operations that can be remotely implemented is a key matter to successfully carry out the RIO protocols. In our resent work [4], we obtained their general and explicit forms. Moreover, we provided evidence of the uniqueness and optimization of our restricted sets based on the precondition that our protocol only uses N maximally entangled states. It must be emphasized that before the beginning of our protocols, we have to build two mapping tables, one of them provides one-to-one mapping from $T_N^r(x) \in \mathbb{T}_N^r$ to the classical information x which is known by the senders, the other one provides one-to-one mapping from a classical information x to $R_N(x)$ which is known by the receiver. Since the unified recovery operations are obtained, all of quantum operations belonging to our restricted sets can be remotely implemented via our protocols in a faithful and determined way. In addition, although the important and interesting quantum operations belonging to the restricted sets should be unitary, but this limitation does not affect our protocol.

In this paper, we not only propose our protocols in detail, but also prove them strictly in the cases of one and more than one qubit. Through respectively describing the cases with the one or many controllers as well as with one or two senders, we explain clearly their roles in our protocols.

It should be pointed out that the implementations of $R_N(x)$ are important in our protocols. It is a key to design a recovery quantum circuits in the near future. In principle, we can construct $R_N(x)$ by using a series of universal

gates [20]. In special, we have found that $R_2(x)$ can be constructed by $C^{\rm not}$ and σ_x [21]:

$$
\begin{aligned}
R_2(1) &= I_{Y_1}\otimes I_{Y_2}, && (90)\\
R_2(2) &= C^{\rm not}(Y_1,Y_2), && (91)\\
R_2(3) &= C^{\rm not}(Y_2,Y_1)C_{not}(Y_1,Y_2)C^{\rm not}(Y_2,Y_1) && (92)\\
R_2(4) &= C^{\rm not}(Y_2,Y_1)C^{\rm not}(Y_1,Y_2), && (93)\\
R_2(5) &= C^{\rm not}(Y_1,Y_2)C^{\rm not}(Y_2,Y_1), && (94)\\
R_2(6) &= C^{\rm not}(Y_2,Y_1), && (95)\\
R_2(7) &= C^{\rm not}(Y_1,Y_2)(I\otimes\sigma_1), && (96)\\
R_2(8) &= (I\otimes\sigma_1), && (97)\\
R_2(9) &= (\sigma_1\otimes I)C^{\rm not}(Y_1,Y_2)C^{\rm not}(Y_2,Y_1), && (98)\\
R_2(10) &= C^{\rm not}(Y_2,Y_1)(I\otimes\sigma_1), && (99)\\
R_2(11) &= C^{\rm not}(Y_2,Y_1)(\sigma_1\otimes I)C^{\rm not}(Y_1,Y_2)C^{\rm not}(Y_2,Y_1), && (100)\\
R_2(12) &= C^{\rm not}(Y_2,Y_1)C^{\rm not}(Y_1,Y_2)(I\otimes\sigma_1), && (101)\\
R_2(13) &= C^{\rm not}(Y_2,Y_1)C^{\rm not}(Y_1,Y_2)(\sigma_1\otimes I), && (102)\\
R_2(14) &= C^{\rm not}(Y_2,Y_1)C^{\rm not}(Y_1,Y_2)(\sigma_1\otimes I)C^{\rm not}(Y_2,Y_1), && (103)\\
R_2(15) &= C^{\rm not}(Y_2,Y_1)(\sigma_1\otimes I), && (104)\\
R_2(16) &= C^{\rm not}(Y_1,Y_2)(\sigma_1\otimes I)C^{\rm not}(Y_2,Y_1), && (105)\\
R_2(17) &= (\sigma_1\otimes I), && (106)\\
R_2(18) &= C^{\rm not}(Y_1,Y_2)(\sigma_1\otimes I), && (107)\\
R_2(19) &= (I\otimes\sigma_1)C^{\rm not}(Y_2,Y_1), && (108)\\
R_2(20) &= C^{\rm not}(Y_1,Y_2)(I\otimes\sigma_1)C^{\rm not}(Y_2,Y_1), && (109)\\
R_2(21) &= C^{\rm not}(Y_2,Y_1)(\sigma_1\otimes I)C^{\rm not}(Y_1,Y_2), && (110)\\
R_2(22) &= C^{\rm not}(Y_2,Y_1)C^{\rm not}(Y_1,Y_2)(I\otimes\sigma_1)C^{\rm not}(Y_2,Y_1), && (111)\\
R_2(23) &= (\sigma_1\otimes I)C^{\rm not}(Y_1,Y_2), && (112)\\
R_2(24) &= (\sigma_1\otimes\sigma_1). && (113)
\end{aligned}
$$

where $C^{\rm not}(Y_1,Y_2)$ means that we use qubit Y_1 as the control qubit, Y_2 as the target qubit to do the control-NOT transformation, and $C^{\rm not}(Y_2,Y_1)$ means we use qubit Y_2 as the control qubit and qubit Y_1 as the target qubit. Furthermore, we are interesting in the construction of a unified recovery quantum circuit, which will be studied in our other manuscript. It is worthy pointing out that the unified recovery operations in our protocols imply that quantum operations that can be remotely implemented can belong to all of the restricted sets but not only a kind of restricted set. This advantage obviously reveals that the power of remote implementations of quantum operations in our protocols is enhanced.

Form the controlled RIOs, we have seen that the controller(s) is (are) an (a group of) administrator(s) in our protocols. If the controllers (controller) accept(s) the application of remote implementations of operations from sender and receiver, or intend(s) to let sender(s) and receiver(s) carry out the RIO task, they (he/she) will perform the startup operation (controlling step) and then transfer the classical information as a "password" to the sender(s) (allowing step) or the receiver so that the protocols can begin and be faithfully completed. When controllers, a sender and a receiver share N GHZ states, it does not mean that the sender and receiver can carry out RIO protocols. This is because that the quantum channel between the sender and receiver has not been opened. The startup of the quantum channel is obtained by the controllers' operation. It is just one of reasons why we use the name of controller(s). Then, the controller(s) transfers his/her classical information as a "password". However, as soon as the password is transferred, the controller has no any means to stop the protocols. Therefore, we suggest a scheme to delay this transmission (password distributing) and send the password(s) to the receiver until the finishing of the receiver's standard recovered step so that the controller(s) keeps his/her's interrupting right up to the end of the protocols, that is, "saying last word". However, it is possible to lead to a little complicated form of the receiver's recovery operation for the multiqubits cases, so we may give up this kind of scheme and put the additional recovery operation before the standard recovery operations.

It should be pointed out that when three partite subsystems share N GHZ states, their position and right are symmetric. Therefore, any partite subsystem can be one of controller, sender and receiver. The controller is determined by the other two parties' choice based on their requirement of RIO, and/or his/her own decision in order to authorize the other two partite subsystems carrying out RIO. If an advanced administrator nominates a controller, he/she can

demand this controller to open the quantum channel between the other two partite subsystems but keep the classical information in hands as a controlled means. If the number of shared GHZ states is n less than N, only two partite subsystems will be symmetric and they can choose as either of a sender and a receiver, the other one partite subsystem with n qubits only can play the controllers.

For the combined remote implementation of quantum operations, we also have displayed that two senders respectively complete the remote implementations of two parts of a quantum operation and then combine them together to obtain the finally remote implementation of the whole quantum operations via GHZ states. Because the second sender has to know the classical information from the first sender, the combination of two parts of operations has a sequence. This implies that the cooperation of all the senders are needed. It is clear that the security of remote implementations of operations is enhanced. The related reasons have been stated in the introduction. This advantage does not exist in the RIO protocol with two senders using two Bell states. In practice, it is possible that different senders have different operational resources and different operational rights, therefore, we can set a suitable combination of their resource and right. It implies that the combined remote implementation can overcome the senders's possible shortcoming and help us to farthest arrive at the power of our protocols in theory. In addition, it is interesting to study the quantum resource cost in the RIO protocol with two senders by comparing the different schemes using one GHZ state with using two Bell state.

Furthermore, if we wish to consider our protocols with more than two senders, or both many controllers and many senders, then the entangled states of three partite subsystems are not enough when only using N GHZ states in order to remotely implement the operations of N qubits. In general, for the cases of quantum operations of N qubits, if there are n $(\leq N))$ controllers and m $(\leq N))$ senders, we need using N EPR-GHZ states at least with $m+n+1$ partite subsystems.

In summary, using GHZ states in the RIOs protocols indeed can enhance their security, increase their variety, extend their possible applications, and even advance their efficiency. These advantages can not be replaced by using Bell states. Therefore, we can say the different quantum resources have the different features and purposes in quantum information processing and communications.

Acknowledgments

We are grateful all the collaborators of our quantum theory group in the institute for theoretical physics of our university. This work was funded by the National Fundamental Research Program of China under No. 2001CB309310, partially supported by the National Natural Science Foundation of China under Grant No. 60573008.

APPENDIX A: SWAPPING TRANSFORMATION

In this appendix, we first study the general swapping transformations, which are the combinations of a series of usual swapping transformations. They are used in our protocols in order to express our formula clearly and compactly, and prove our protocols more easily.

Note that a swapping transformation of two neighbor qubits is defined by

$$S_W = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \tag{A1}$$

Its action is

$$S_W|\alpha_X\beta_Y\rangle = |\beta_Y\alpha_X\rangle, \quad S_W(M^X\otimes M^Y)S_W = M^Y\otimes M^X. \tag{A2}$$

This means that the swapping transformation changes the space structure $H_X\otimes H_Y$ into $H_Y\otimes H_X$.

For an N-qubit system, the swapping gate of the ith qubit and the $(i+1)$th qubit reads

$$S_N(i,i+1) = \sigma_0^{\otimes(i-1)}\otimes S_W\otimes\sigma_0^{\otimes(N-i-1)}. \tag{A3}$$

Two rearranged transformations are defined by

$$F_N(i,j) = \prod_{\alpha=1\leftarrow}^{j-i} S_N(j-\alpha, j+1-\alpha) \tag{A4}$$

$$P_N(j,k)=\prod_{\beta=j\leftarrow}^{k-1} S_N(\beta,\beta+1) \tag{A5}$$

where $F_N(i,j)$ extracts out the spin-state of site j, and rearranges it forwards to the site i $(i<j)$ in the qubit-string, where $P_N(j,k)$ extracts out the spin-state of site j, and rearranges it backwards to the site k $(k>j)$ in the qubit-string. Note that "$\leftarrow$" means that the factors are arranged from right to left corresponding to α,β from small to large. Now, in terms of $P(j,k)$, we can introduce two general swapping transformations with the forms

$$\Lambda(2,N)=\prod_{i=1\leftarrow}^{N-1} P_{2N}\left(2(N-i),2N-i\right), \quad (N\geq 2), \tag{A6}$$

$$\Omega(2,N)=\prod_{i=1\leftarrow}^{N} P_{2N}\left(1,2N\right), \quad (N\geq 2). \tag{A7}$$

Thus,

$$\Lambda(2,N)\left(\bigotimes_{i=1}^{N}|a_ib_i\rangle\right)=\left(\bigotimes_{i=1}^{N}|a_i\rangle\right)\otimes\left(\bigotimes_{j=1}^{N}|b_j\rangle\right), \tag{A8}$$

$$\Lambda(2,N)\left(\bigotimes_{k=1}^{N}\left(M_{\alpha_i}^{A_i}\otimes M_{\beta_i}^{B_i}\right)\right)\Lambda^{-1}(2,N)=\left(\bigotimes_{i=1}^{N}M_{\alpha_i}^{A_i}\right)\otimes\left(\bigotimes_{j=1}^{N}M_{\beta_j}^{B_j}\right), \tag{A9}$$

$$\Omega(2,N)\left[\left(\bigotimes_{i=1}^{N}|a_i\rangle\right)\otimes\left(\bigotimes_{j=1}^{N}|b_j\rangle\right)\right]=\left(\bigotimes_{i=1}^{N}|b_i\rangle\right)\otimes\left(\bigotimes_{j=1}^{N}|a_j\rangle\right), \tag{A10}$$

$$\Omega(2,N)\left[\left(\bigotimes_{i=1}^{N}M_{\alpha_i}^{A_i}\right)\left(\bigotimes_{i=1}^{N}M_{\beta_i}^{B_i}\right)\right]\Omega^{-1}(2,N)=\left(\bigotimes_{i=1}^{N}M_{\beta_i}^{B_i}\right)\otimes\left(\bigotimes_{j=1}^{N}M_{\alpha_j}^{A_j}\right). \tag{A11}$$

Similarly, we can introduce

$$\Upsilon(3,N)=\prod_{i=1\leftarrow}^{N-1} F_{3N}\left(3i,2N+i\right), \quad (N\geq 2); \tag{A12}$$

$$\Upsilon(4,N)=\prod_{i=1\leftarrow}^{N-1} F_{4N}\left(4i,3N+i\right), \quad (N\geq 2). \tag{A13}$$

$$\Gamma(3,N)=\left(I_{2^N}\otimes\Omega(2,N)\right)\left(\Lambda(2,N)\otimes I_{2^N}\right). \tag{A14}$$

Thus,

$$\Upsilon(3,N)\left(\bigotimes_{i=1}^{N}|a_ib_i\rangle\right)\otimes\left(\bigotimes_{j=1}^{N}|k_j\rangle\right)=\bigotimes_{i=1}^{N}|a_ib_ik_i\rangle, \tag{A15}$$

$$\Upsilon(3,N)\left[\bigotimes_{k=1}^{N}\left(M_{\alpha_i}^{A_i}\otimes M_{\beta_i}^{B_i}\right)\right]\left(\bigotimes_{j=1}^{N}M_{\gamma_j}^{Y_j}\right)\Upsilon^{-1}(3,N)=\bigotimes_{i=1}^{N}\left(M_{\alpha_i}^{A_i}\otimes M_{\beta_i}^{B_i}\otimes M_{\gamma_i}^{Y_i}\right). \tag{A16}$$

$$\Upsilon(4,N)\left(\bigotimes_{i=1}^{N}|a_ib_ic_i\rangle\right)\otimes\left(\bigotimes_{j=1}^{N}|k_j\rangle\right)=\bigotimes_{i=1}^{N}|a_ib_ic_ik_i\rangle, \tag{A17}$$

$$\Upsilon(4,N)\left[\bigotimes_{k=1}^{N}\left(M_{\alpha_i}^{A_i}\otimes M_{\beta_i}^{B_i}\otimes M_{\gamma_i}^{C_i}\right)\right]\left(\bigotimes_{j=1}^{N}M_{\delta_j}^{Y_j}\right)\Upsilon^{-1}(4,N)=\bigotimes_{i=1}^{N}\left(M_{\alpha_i}^{A_i}\otimes M_{\beta_i}^{B_i}\otimes M_{\gamma_i}^{C_i}\otimes M_{\delta_i}^{Y_i}\right). \tag{A18}$$

$$\Gamma(3,N)\left(\bigotimes_{i=1}^{N}|a_ib_i\rangle\right)\otimes\left(\bigotimes_{j=1}^{N}|k_j\rangle\right)=\left(\bigotimes_{i=1}^{N}|a_i\rangle\right)\otimes\left(\bigotimes_{j=1}^{N}|k_j\rangle\right)\otimes\left(\bigotimes_{k=1}^{N}|b_k\rangle\right), \tag{A19}$$

$$\begin{aligned}&\Gamma(3,N)\left[\bigotimes_{k=1}^{N}\left(M_{\alpha_i}^{A_i}\otimes M_{\beta_i}^{B_i}\right)\right]\left(\bigotimes_{j=1}^{N}M_{\gamma_j}^{Y_j}\right)\Gamma^{-1}(3,N)\\&=\left(\bigotimes_{i=1}^{N}M_{\alpha_i}^{A_i}\right)\otimes\left(\bigotimes_{j=1}^{N}M_{\gamma_j}^{Y_j}\right)\otimes\left(\bigotimes_{k=1}^{N}M_{\beta_k}^{B_k}\right).\end{aligned} \tag{A20}$$

For the cases with n GHZ states and $N-n$ Bell states, we introduce

$$\Omega(3,N)=\left(\Omega(2,N)\otimes I_{2^N}\right)\left(I_{2^N}\otimes\Omega(2,N)\right). \tag{A21}$$

Obviously

$$\Omega(3,N)\left[\left(\bigotimes_{i=1}^{N}|a_ib_i\rangle\right)\otimes\left(\bigotimes_{j=1}^{N}|c_j\rangle\right)\right]=\left(\bigotimes_{i=1}^{N}|c_i\rangle\right)\otimes\left(\bigotimes_{j=1}^{N}|a_jb_j\rangle\right), \tag{A22}$$

$$\Omega(3,N)\left\{\left[\bigotimes_{i=1}^{N}\left(M_{\alpha_i}^{A_i}\otimes M_{\beta_i}^{B_i}\right)\right]\left(\bigotimes_{i=1}^{N}M_{\gamma_i}^{C_i}\right)\right\}\Omega^{-1}(3,N)=\left(\bigotimes_{i=1}^{N}M_{\gamma_i}^{C_i}\right)\otimes\left[\bigotimes_{j=1}^{N}\left(M_{\alpha_j}^{A_j}\otimes M_{\beta_j}^{B_j}\right)\right]. \tag{A23}$$

More generally, consider the set $\mathbb{Q}_N$ to be a whole permutation of the bit-string $a_1a_2\cdots a_N$, and denote the z element with a bit-string form $Q(z)=q_1(z)q_2(z)\cdots q_N(z)$, we always can obtain such a general swapping transformation W_N that a computational basis $|a_1a_2\cdots a_N\rangle$ of N-qubit systems can be swapped as another basis $|q_1(z)q_2(z)\cdots q_N(z)\rangle$ in which $q_1(z)q_2(z)\cdots q_N(z)$ is an arbitrary element of $\mathbb{Q}_N$. Thus, we can write a given general swapping transformation $W_N\left(a_1a_2\cdots a_N\to q_1(z)q_2(z)\cdots q_N(z)\right)$,

$$W_N\left[a_1a_2\cdots a_N\to q_1(z)q_2(z)\cdots q_N(z)\right]|a_1a_2\cdots a_N\rangle=|q_1(z)q_2(z)\cdots q_N(z)\rangle. \tag{A24}$$

Furthermore, if we denote two dimensional space A_i spanned by $|a_i\rangle$ ($a_i=0,1$ and $i=1,2,\cdots N$), while M^{A_i} is a matrix belonging to this space, we obviously have

$$W_N^{-1}\left[a_1a_2\cdots a_N\to q_1(z)q_2(z)\cdots q_N(z)\right]\left(\prod_{i=1}^{N}M^{A_i}\right)W_N\left[a_1a_2\cdots a_N\to q_1(z)q_2(z)\cdots q_N(z)\right]=\left(\prod_{i=1}^{N}M^{A_{q_i(z)}}\right). \tag{A25}$$

Therefore, the general swapping transformation W_N defined above can be used to change the space structure of multiqubits systems.

APPENDIX B: THE PROOF OF OUR PROTOCOL IN THE CASES MORE THAN ONE QUBIT

Here, we would like to prove our protocols of controlled and combined RIO belonging to our restricted sets in the cases of more than one qubit.

For the cases with n controllers, since

$$(I_4 \otimes |c\rangle\langle c|H)\,|\mathrm{GHZ}_+\rangle = \frac{1}{2}\left(|00\rangle + (-1)^c|11\rangle\right) \otimes |c\rangle. \tag{B1}$$

The initial state is transformed as

$$\left|\Psi_N^C\right\rangle \;=\; \mathcal{C}(c_1, c_2, \cdots, c_n)\left|\Psi_N^{\mathrm{ini}}\right\rangle = \frac{1}{\sqrt{2^n}}\left(\bigotimes_{m=1}^{n}|\mathrm{Bell}_{\mathrm{c_m}}\rangle_{A_m B_m} \otimes |c_m\rangle\right)\left(\bigotimes_{s=n+1}^{N}|\mathrm{Bell}_+\rangle_{A_j B_j}\right) \otimes |\xi\rangle_{y_1\cdots y_N}, \tag{B2}$$

where

$$|\mathrm{Bell}_{\mathrm{c_i}}\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + (-1)^{c_i}|11\rangle\right). \tag{B3}$$

Again introducing the swapping transformation

$$\Xi_N(n) = \left[I_n \otimes \Upsilon(3, N)\right]\Theta_C^{-1}(n), \tag{B4}$$

where $\Upsilon(3, N)$ and $\Theta_C(n)$ is defined as above, we can rewrite

$$\begin{aligned}
\left|\Psi_N^C\right\rangle \;&=\; \frac{1}{\sqrt{2^{N+n}}}\Xi_N(n)\left(\bigotimes_{i=1}^{n}|c_i\rangle\right)\sum_{k_1,\cdots k_N=0}^{1} y_{k_1\cdots k_N} \\
&\quad \bigotimes_{m=1}^{n}\left(\mathfrak{r}(c_i)\otimes I_4\right)\Big(|00k_m\rangle_{A_m B_m y_m} + (-1)^{c_m}|11k_m\rangle_{A_m B_m y_m}\Big) \qquad \text{(B5)}\\
&\quad \bigotimes_{s=n+1}^{N}\left(|00k_s\rangle_{A_s B_s Y_s} + |11k_s\rangle_{A_s B_s Y_s}\right) \\
&=\; \frac{1}{\sqrt{2^{N+n}}}\Xi_N(n)\left(\bigotimes_{i=1}^{n}|c_i\rangle\right)\sum_{k_1,\cdots k_N=0}^{1} y_{k_1\cdots k_N} \\
&\quad \bigotimes_{m=1}^{n}\left(I_2\otimes\mathfrak{r}(c_i)\otimes I_2\right)\Big(|00k_m\rangle_{A_m B_m y_m} + (-1)^{c_m}|11k_m\rangle_{A_m B_m y_m}\Big) \qquad \text{(B6)}\\
&\quad \bigotimes_{s=n+1}^{N}\left(|00k_s\rangle_{A_s B_s Y_s} + |11k_s\rangle_{A_s B_s Y_s}\right). \qquad \text{(B7)}
\end{aligned}$$

Since $\mathfrak{r}(c_i)\mathfrak{r}(c_i) = I_2$, therefore, whatever Charlies transfer their information to Alice or Bob, all factors $\mathfrak{r}(c_i)$ will be eliminated because the product of it and the prior transformation $\mathfrak{r}(c_i)$ gets 1. If we delay the controllers' information to after the preparing, then we can similarly discuss in terms of Eq. (19). If we delay the controllers' information to the end of our protocols (that is "say last word") in the cases of multiqubits, we will pay the price that a more complicated additionally recovery operation is resulted in. In the following, for simplicity, we only prove the case that Charlies' information is transferred to Bob. The other kinds of our protocols can be proved similar to the cases of one qubit.

From Bob's preparing (after his prior operation), it follows that

$$\begin{aligned}\left|\Psi^P(b_1,\cdots b_N)\right\rangle &= \mathcal{P}_B(b_1,b_2,\cdots,b_N)\mathcal{P}_B^{\rm add}(c_1,c_2,\cdots,c_n)\left|\Psi_N^C\right\rangle \\ &= \frac{1}{\sqrt{2^{N+n}}}\Xi_N(n)\left(\bigotimes_{m=1}^{n}|c_m\rangle\right)\sum_{k_1,\cdots k_N=0}^{1} y_{k_1\cdots k_N}\bigotimes_{s=1}^{N} \\ &\quad\times\left[\sigma_0\left(\otimes|b_s\rangle\langle b_s|\otimes\sigma_0\right)C^{\rm not}(2,1)\right]\left(|00k_s\rangle_{A_sB_sY_s}+|11k_s\rangle_{A_sB_sY_s}\right) \\ &= \frac{1}{\sqrt{2^{N+n}}}\Xi_N(n)\left(\bigotimes_{m=1}^{n}|c_m\rangle\right)\left[\bigotimes_{s=1}^{N}(\sigma_{b_s}\otimes\sigma_0)\otimes I_{2^N}\right] \\ &\quad\times\sum_{k_1,\cdots k_N=0}^{1} y_{k_1\cdots k_N}\bigotimes_{t=1}^{N}|k_tb_tk_t\rangle_{A_tB_tY_t},\end{aligned}\tag{B8}$$

where we have used Eq. (37)

Actually, the physical idea to design our protocol is to perfectly prepare the state of joint system being in the correlated superposition. If there is the controller(s), the whole preparing is completed by the controller's startup, receiver's setting and sender's assistance, that $\mathcal{P}=\mathcal{P}_S\mathcal{P}_B\mathcal{P}_B^{\rm add}\mathcal{C}$. It is easy to see that

$$\begin{aligned}\left|\Psi_f^{\rm P}\right\rangle &= \mathcal{P}_S\left|\Psi^{\rm ini}\right\rangle = \frac{1}{\sqrt{2^{N+n}}}\Xi_N(n)\left(\bigotimes_{m=1}^{n}|c_m\rangle\right)\otimes\sum_{k_1,\cdots k_N=0}^{1} y_{k_1\cdots k_N}\bigotimes_{s=1}^{N}|k_sb_sk_s\rangle_{AsB_sy_s} \\ &= \frac{1}{\sqrt{2^{N+n}}}\Xi_N'(n)\left(\bigotimes_{m=1}^{n}|c_m\rangle\right)\otimes\sum_{k_1,\cdots k_N=0}^{1} y_{k_1\cdots k_N}\left(\bigotimes_{s=1}^{N}|k_s\rangle_{A_s}\right) \\ &\quad\otimes\left(\bigotimes_{s=1}^{N}|k_s\rangle_{Y_s}\right)\left(\bigotimes_{t=1}^{N}|b_t\rangle_{B_t}\right),\end{aligned}\tag{B9}$$

where we have defined

$$\Xi_N'(n)=\Xi_N(n)\left[I_{2^n}\otimes\Upsilon^{-1}(3,N)\Gamma^{-1}(3,N)\right].\tag{B10}$$

For simplicity, we only need to consider the subspace $A_1A_2\cdots A_NY_1Y_2\cdots Y_N$, and omit the general swapping transformation as well as the coefficient, we rewrite

$$\left|\psi_f^{\rm P}\right\rangle\propto\sum_{k_1,\cdots k_N=0}^{1} y_{k_1\cdots k_N}\left(\bigotimes_{m=1}^{N}|k_m\rangle_{A_m}\right)\otimes\left(\bigotimes_{m=1}^{N}|k_m\rangle_{Y_m}\right).\tag{B11}$$

Thus, Alice's sending step and Bob's recovery operations yield the final state in our interesting subsystem as

$$\begin{aligned}\left|\psi_N^{\rm final}\right\rangle &\propto \bigotimes_{m=1}^{N}|a_m\rangle_{A_m}\otimes\sum_{k_1,\cdots k_N=0}^{1} y_{k_1\cdots k_N} \\ &\quad\times\left[\left(\bigotimes_{m=1}^{N}\langle a_m|\right)\left(\bigotimes_{m=1}^{N}H^{A_m}\right)T_N^r(x,t)\left(\bigotimes_{m=1}^{N}|k_m\rangle\right)\right] \\ &\quad\times\left(\bigotimes_{m=1}^{N}\mathfrak{r}^{Y_m}(a_m)\right)R_N(x)\left(\bigotimes_{m=1}^{N}|k_m\rangle_{Y_m}\right).\end{aligned}\tag{B12}$$

It is a key matter that we can prove the relation

$$T_N^r(1)R_N(x)=\sum_{m=1}^{2^N}t_m|i,D\rangle\langle m,D|\sum_{n=1}^{2^N}|n,D\rangle\langle p_n(x),D|=\sum_{m=1}^{2^N}t_m|m,D\rangle\langle p_m(x),D|=T_N^r(x),\tag{B13}$$

and we have known that

$$T_N^r(1)=\sum_{j_1,\cdots,j_N=0}^{1}t_{j_1j_2\cdots j_N}|j_1j_2\cdots j_N\rangle\langle j_1j_2\cdots j_N|,\tag{B14}$$

$$\mathfrak{r}(a_m) = \sum_{l_m=0}^{1} (-1)^{a_m l_m} |l_m\rangle\langle l_m|. \tag{B15}$$

Substituting them into (B12), we have

$$\begin{aligned}
\left|\psi_N^{\rm final}\right\rangle \;\propto\; & \bigotimes_{m=1}^{N} |a_m\rangle_{A_m} \otimes \left\{ \sum_{j_1,\cdots,j_N}^{1} \sum_{k_1,\cdots k_N=0}^{1} \sum_{l_1,\cdots,l_N}^{1} t_{j_1\cdots j_N} y_{k_1\cdots k_N} \right. \\
& \times \left(\prod_{m=1}^{N} \langle a_m|H|j_m\rangle\right) \left[\left(\bigotimes_{m=1}^{N} \langle j_m|\right) R_N(x) \left(\bigotimes_{m=1}^{N} |k_m\rangle_{Y_m}\right)\right] \\
& \times \left[\left(\bigotimes_{m=1}^{N} \langle l_m|\right) R_N(x) \left(\bigotimes_{m=1}^{N} |k_m\rangle_{Y_m}\right)\right] \left(\prod_{m=1}^{N} (-1)^{a_m l_m}\right) \bigotimes_{m=1}^{N} |l_m\rangle_{Y_m}.
\end{aligned} \tag{B16}$$

Because that $R_N(x)$ is such a matrix that its every row and every column only has a nonzero element, we can obtain

$$\begin{aligned}
& \left[\left(\bigotimes_{m=1}^{N} \langle j_m|\right) R_N(x) \left(\bigotimes_{m=1}^{N} |k_m\rangle_{Y_m}\right)\right] \left[\left(\bigotimes_{m=1}^{N} \langle l_m|\right) R_N(x) \left(\bigotimes_{m=1}^{N} |k_m\rangle_{Y_m}\right)\right] \\
= & \left(\prod_{m=1}^{N} \delta_{j_m l_m}\right) \left[\left(\bigotimes_{m=1}^{N} \langle j_m|\right) R_N(x) \left(\bigotimes_{m=1}^{N} |k_m\rangle_{Y_m}\right)\right].
\end{aligned} \tag{B17}$$

Again from

$$\langle a_m|H|j_m\rangle(-1)^{a_m j_m} = \frac{1}{\sqrt{2}}, \tag{B18}$$

we can derive out

$$\begin{aligned}
\left|\psi_N^{\rm final}\right\rangle \;\propto\; & \bigotimes_{m=1}^{N} |a_m\rangle_{A_m} \otimes \left\{ \sum_{j_1,\cdots,j_N}^{1} \sum_{k_1,\cdots k_N=0}^{1} \sum_{l_1,\cdots,l_N}^{1} t_{j_1\cdots j_N} y_{k_1\cdots k_N} \right. \\
& \times \left[\left(\bigotimes_{m=1}^{N} \langle j_m|\right) R_N(x) \left(\bigotimes_{m=1}^{N} |k_m\rangle_{Y_m}\right)\right] \bigotimes_{m=1}^{N} |j_m\rangle_{Y_m}.
\end{aligned} \tag{B19}$$

If we directly act $T_N^r(x,t)$ on the unknown state, we have

$$\begin{aligned}
T_N^r(x,t)|\xi\rangle_{Y_1\cdots Y_N} &= \sum_{k_1,\cdots,k_N=0}^{1} y_{k_1\cdots k_N} T_N^r(1,t) R(x) |k_1 k_2 \cdots k_n\rangle \\
&= \sum_{k_1,\cdots,k_N=0}^{1} \sum_{k_1,\cdots,k_N=0}^{1} t_{j_1\cdots j_N} y_{k_1\cdots k_N} \\
&\quad \times \langle j_1 j_2 \cdots j_N|R(x)|k_1 k_2 \cdots k_n\rangle |j_1 j_2 \cdots j_N\rangle.
\end{aligned} \tag{B20}$$

This means that

$$\left|\psi_N^{\rm final}\right\rangle \propto \bigotimes_{i=1}^{N} |a_i\rangle_{A_i} \otimes \left(T_N^r(x,t)|\xi\rangle_{y_1\cdots y_N}\right). \tag{B21}$$

Finally, we add the other subspaces and restore the structure of Hilbert's space by using the swapping transformations, and then finish the proof of our protocols for the cases with n controllers.

When there are two senders, our protocol is actually the combination of twice remote implementations. However, after the first operation is transferred remotely, the second sender's local system loses perfectly correlation with the

remote system to be operated. Since we use one GHZ state as a quantum channel, the first transfer has not exhausted all of correlation in the joint system. Compared with the cases of one qubit, we can obtain the method to rebuild their correlation through replacing σ_d by the fixed form of the first operation.

To our purpose, let us start with the state prepared by Bob:

$$\begin{aligned}
\left|\Psi_N^P\right\rangle &= \frac{1}{\sqrt{2^N}}\Upsilon^{-1}(4,N)\mathcal{P}_B(b_1,\cdots,b_N)\Upsilon^{-1}(4,N)\left[\sum_{k_1,\cdots,k_N=0}^{1} y_{k_1\cdots k_N}\bigotimes_{m=1}^{N}\left(|000k_m\rangle+|111k_m\rangle\right)\right] \\
&= \frac{1}{\sqrt{2^N}}\Upsilon^{-1}(4,N)\left(\bigotimes_{m=1} F_4^{-1}(1,3)\right)\left\{\bigotimes_{m=1}^{N}\left[I_4\otimes\left(|b_m\rangle\langle b_m|\otimes\sigma_0\right)C^{\rm not}(2,1)\right]\right. \\
&\quad \left.\times\left[|000k_m\rangle_{C_mA_mB_mY_m}+|111k_m\rangle_{C_mA_mB_mY_m}\right]\right\}. \qquad \text{(B22)}
\end{aligned}$$

Using Eq. (52), we have

$$\begin{aligned}
\left|\Psi_N^P\right\rangle &= \frac{1}{\sqrt{2^N}}\Upsilon^{-1}(4,N)\left(\bigotimes_{m=1} F_4^{-1}(1,3)\right) \\
&\quad\times\sum_{k_1\cdots k_N=0}^{1} y_{k_1\cdots k_n}\left[\bigotimes_{m=1}^{N}\left(\sigma_{b_m}\otimes\sigma_{b_m}\otimes I_4\right)|k_mk_mb_mk_m\rangle_{C_mA_mB_mY_m}\right] \\
&= \frac{1}{\sqrt{2^N}}\sum_{k_1\cdots k_N=0}^{1} y_{k_1\cdots k_n}\left[\bigotimes_{m=1}^{N}\left(\sigma_{b_m}\otimes\sigma_0\otimes\sigma_{b_m}\right)|k_mb_mk_m\rangle_{A_mB_mC_m}\right]\otimes\left(\bigotimes_{m=1}^{N}|k_m\rangle_{Y_m}\right) \\
&= \frac{1}{\sqrt{2^N}}\left(\Lambda(2,N)\otimes I_{4^N}\right)\left(\Gamma^{-1}(3,N)\otimes I_{2^N}\right)\sum_{k_1\cdots k_N=0}^{1} y_{k_1\cdots k_n}\left(\bigotimes_{m=1}^{N}\sigma_{b_m}|k_m\rangle_{A_m}\right) \\
&\quad\otimes\left(\bigotimes_{m=1}^{N}|b_m\rangle_{B_m}\right)\otimes\left(\bigotimes_{m=1}^{N}\sigma_{b_m}|k_m\rangle_{C_m}\right)\otimes\left(\bigotimes_{m=1}^{N}|k_m\rangle_{Y_m}\right). \qquad \text{(B23)}
\end{aligned}$$

Omitting the swapping transformations as well as coefficient and keeping the relevant subspaces, we have

$$\left|\psi_N^P\right\rangle \propto \sum_{k_1\cdots k_N=0}^{1} y_{k_1\cdots k_n}\left(\bigotimes_{m=1}^{N}\sigma_{b_m}|k_m\rangle_{A_m}\right)\otimes\left(\bigotimes_{m=1}^{N}\sigma_{b_m}|k_m\rangle_{C_m}\right)\otimes\left(\bigotimes_{m=1}^{N}|k_m\rangle_{Y_m}\right). \qquad \text{(B24)}$$

Alice's sending, Charlie's sending and Bob's recovery operations lead to

$$\begin{aligned}
\left|\psi_N^{\rm final}\right\rangle &\propto \left(\bigotimes_{m=1}^{N}|a_m\rangle_{A_m}\right)\otimes\left(\bigotimes_{m=1}^{N}|c_m\rangle_{C_m}\right) \\
&\quad\times\sum_{k_1\cdots k_N=0}^{1} y_{k_1\cdots k_n}\left[\left(\bigotimes_{m=1}^{N}\langle a_m|\right)\left(\bigotimes_{m=1}^{N}H\right)T_N^r(x,u)\left(\bigotimes_{m=1}^{N}|k_m\rangle\right)\right] \\
&\quad\times\left[\left(\bigotimes_{m=1}^{N}\langle b_m|\right)\left(\bigotimes_{m=1}^{N}H\right)T_N^r(y,v)R_N(x)\left(\bigotimes_{m=1}^{N}|k_m\rangle\right)\right] \\
&\quad\otimes\left[\left(\bigotimes_{m=1}^{N}\mathfrak{r}(b_m)\right)R_N(y)\left(\bigotimes_{m=1}^{N}\mathfrak{r}(a_m)\right)R_N(x)\left(\bigotimes_{m=1}^{N}|k_m\rangle_{Y_m}\right)\right]. \qquad \text{(B25)}
\end{aligned}$$

Now, we have seen that it is similar to the cases of one qubit as well as the cases of multiqubits with the controllers,

the proof skills have been shown in the last of Secs. III and IV. Firstly, in terms of Eqs.(B14) and (B15), we have

$$\begin{aligned}\left|\psi_N^{\text{final}}\right\rangle \propto & \left(\bigotimes_{m=1}^{N}\left|a_m\right\rangle_{A_m}\right)\otimes\left(\bigotimes_{m=1}^{N}\left|c_m\right\rangle_{C_m}\right)\sum_{j_1\cdots j_N=0}^{1}\sum_{k_1\cdots k_N=0}^{1}\sum_{l_1\cdots l_N=0}^{1}u_{j_1\cdots j_N}y_{k_1\cdots k_n}\\ & \times\left[\left(\bigotimes_{m=1}^{N}\left\langle a_m\right|\right)\left(\bigotimes_{m=1}^{N}H\right)\left(\bigotimes_{m=1}^{N}\left|j_m\right\rangle\right)\left(\prod_{m=1}^{N}(-1)^{a_m l_m}\right)\right]\\ & \times\left[\left(\bigotimes_{m=1}^{N}\left\langle j_m\right|\right)R_N(x)\left(\bigotimes_{m=1}^{N}\left|k_m\right\rangle\right)\right]\left[\left(\bigotimes_{m=1}^{N}\left\langle l_m\right|\right)R_N(x)\left(\bigotimes_{m=1}^{N}\left|k_m\right\rangle\right)\right]\\ & \times\left[\left(\bigotimes_{m=1}^{N}\left\langle b_m\right|\right)\left(\bigotimes_{m=1}^{N}H\right)T_N^r(y,v)R_N(x)\left(\bigotimes_{m=1}^{N}\left|k_m\right\rangle\right)\right]\\ & \otimes\left[\left(\bigotimes_{m=1}^{N}\mathfrak{r}(b_m)\right)R_N(y)\left(\bigotimes_{m=1}^{N}\left|l_m\right\rangle_{Y_m}\right)\right].\end{aligned}\tag{B26}$$

Secondly, from the Eqs.(B17) and (B18), it follows that

$$\begin{aligned}\left|\psi_N^{\text{final}}\right\rangle \propto & \left(\bigotimes_{m=1}^{N}\left|a_m\right\rangle_{A_m}\right)\otimes\left(\bigotimes_{m=1}^{N}\left|c_m\right\rangle_{C_m}\right)\sum_{j_1\cdots j_N=0}^{1}\sum_{k_1\cdots k_N=0}^{1}u_{j_1\cdots j_N}y_{k_1\cdots k_n}\\ & \times\left[\left(\bigotimes_{m=1}^{N}\left\langle j_m\right|\right)R_N(x)\left(\bigotimes_{m=1}^{N}\left|k_m\right\rangle\right)\right]\left[\left(\bigotimes_{m=1}^{N}\left\langle b_m\right|\right)\left(\bigotimes_{m=1}^{N}H\right)T_N^r(y,v)R_N(x)\left(\bigotimes_{m=1}^{N}\left|k_m\right\rangle\right)\right]\\ & \otimes\left[\left(\bigotimes_{m=1}^{N}\mathfrak{r}(b_m)\right)R_N(y)\left(\bigotimes_{m=1}^{N}\left|j_m\right\rangle_{Y_m}\right)\right].\end{aligned}\tag{B27}$$

Thirdly, inserting the complete relation after $T_N^r(y)$ and using Eq. (B17), we will eliminate a $R_N(x)$

$$\begin{aligned}\left|\psi_N^{\text{final}}\right\rangle \propto & \left(\bigotimes_{m=1}^{N}\left|a_m\right\rangle_{A_m}\right)\otimes\left(\bigotimes_{m=1}^{N}\left|c_m\right\rangle_{C_m}\right)\sum_{j_1\cdots j_N=0}^{1}\sum_{k_1\cdots k_N=0}^{1}u_{j_1\cdots j_N}y_{k_1\cdots k_n}\\ & \times\left[\left(\bigotimes_{m=1}^{N}\left\langle j_m\right|\right)R_N(x)\left(\bigotimes_{m=1}^{N}\left|k_m\right\rangle\right)\right]\left[\left(\bigotimes_{m=1}^{N}\left\langle b_m\right|\right)\left(\bigotimes_{m=1}^{N}H\right)T_N^r(y,v)\left(\bigotimes_{m=1}^{N}\left|j_m\right\rangle\right)\right]\\ & \otimes\left[\left(\bigotimes_{m=1}^{N}\mathfrak{r}(b_m)\right)R_N(y)\left(\bigotimes_{m=1}^{N}\left|j_m\right\rangle_{Y_m}\right)\right].\end{aligned}\tag{B28}$$

Fourthly, substituting Eqs.(B14) and (B15) gives

$$\begin{aligned}\left|\psi_N^{\text{final}}\right\rangle \propto & \left(\bigotimes_{m=1}^{N}\left|a_m\right\rangle_{A_m}\right)\otimes\left(\bigotimes_{m=1}^{N}\left|c_m\right\rangle_{C_m}\right)\sum_{i_1\cdots i_N=0}^{1}\sum_{j_1\cdots j_N=0}^{1}\sum_{k_1\cdots k_N=0}^{1}\sum_{l_1\cdots l_N=0}^{1}v_{i_1\cdots i_N}u_{j_1\cdots j_N}y_{k_1\cdots k_n}\\ & \times\left[\left(\bigotimes_{m=1}^{N}\left\langle j_m\right|\right)R_N(x)\left(\bigotimes_{m=1}^{N}\left|k_m\right\rangle\right)\right]\left[\left(\bigotimes_{m=1}^{N}\left\langle b_m\right|\right)\left(\bigotimes_{m=1}^{N}H\right)\left(\bigotimes_{m=1}^{N}\left|i_m\right\rangle\right)\right]\left(\prod_{m=1}^{N}(-1)^{b_m l_m}\right)\\ & \times\left[\left(\bigotimes_{m=1}^{N}\left\langle i_m\right|\right)R_N(y)\left(\bigotimes_{m=1}^{N}\left|j_m\right\rangle\right)\right]\left[\left(\bigotimes_{m=1}^{N}\left\langle l_m\right|\right)R_N(y)\left(\bigotimes_{m=1}^{N}\left|j_m\right\rangle\right)\right]\otimes\left(\bigotimes_{m=1}^{N}\left|l_m\right\rangle_{Y_m}\right).\end{aligned}\tag{B29}$$

Finally, from Eqs.(B17) and (B18), it follows that

$$\begin{aligned}
\left|\psi_N^{\text{final}}\right\rangle &\propto \left(\bigotimes_{m=1}^N |a_m\rangle_{A_m}\right)\otimes\left(\bigotimes_{m=1}^N |c_m\rangle_{C_m}\right)\sum_{i_1\cdots i_N=0}^{1}\sum_{j_1\cdots j_N=0}^{1}\sum_{k_1\cdots k_N=0}^{1} v_{i_1\cdots i_N}u_{j_1\cdots j_N}y_{k_1\cdots k_n}\\
&\quad\times\left[\left(\bigotimes_{m=1}^N\langle j_m|\right)R_N(x)\left(\bigotimes_{m=1}^N|k_m\rangle\right)\right]\left[\left(\bigotimes_{m=1}^N\langle i_m|\right)R_N(y)\left(\bigotimes_{m=1}^N|j_m\rangle\right)\right]\otimes\left(\bigotimes_{m=1}^N|i_m\rangle_{Y_m}\right)\\
&= \left(\bigotimes_{m=1}^N |a_m\rangle_{A_m}\right)\otimes\left(\bigotimes_{m=1}^N |c_m\rangle_{C_m}\right)\otimes T_N^r(y,v)T_N^r(x,u)|\xi\rangle_{Y_1\cdots Y_N},
\end{aligned}\tag{B30}$$

where we have used the fact that

$$\begin{aligned}
T_N^r(y,v)T_N^r(x,u)|\xi\rangle_{Y_1\cdots Y_N} &= \sum_{j_1,\cdots,j_N=0}^{1}\sum_{k_1,\cdots,k_N=0}^{1} u_{j_1\cdots j_N}y_{k_1\cdots k_N}\\
&\quad\times\left[\left(\bigotimes_{m=1}^N\langle j_m|\right)R_N(x)\left(\bigotimes_{m=1}^N|k_m\rangle\right)\right]T_N^r(y,v)\left(\bigotimes_{m=1}^N|j_m\rangle_{Y_m}\right)\\
&= \sum_{i_1\cdots i_N=0}^{1}\sum_{j_1\cdots j_N=0}^{1}\sum_{k_1\cdots k_N=0}^{1} v_{i_1\cdots i_N}u_{j_1\cdots j_N}y_{k_1\cdots k_n}\left[\left(\bigotimes_{m=1}^N\langle j_m|\right)R_N(x)\left(\bigotimes_{m=1}^N|k_m\rangle\right)\right]\\
&\quad\times\left[\left(\bigotimes_{m=1}^N\langle i_m|\right)R_N(y)\left(\bigotimes_{m=1}^N|j_m\rangle\right)\right]\otimes\left(\bigotimes_{m=1}^N|i_m\rangle_{Y_m}\right).
\end{aligned}\tag{B31}$$

Therefore, after restoring the coefficient, adding the other subspaces and rearranging the space structure, we finish the proof of our protocol with two senders in the cases of N qubits.

---

[1] C.H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993)
[2] S. F. Huelga, J. A. Vaccaro, A. Chefles, and M. B. Plenio, Phys. Rev. A **63**, 042303 (2001)
[3] S. F. Huelga, M. B. Plenio, and J. A. Vaccaro, Phys. Rev. A **65**, 042316 (2002)
[4] An Min Wang, Phys. Rev. A, **74** 032317 (2006); quant-ph/0510209
[5] J. I. Cirac, A. K. Ekert, S. F. Huelga, and C. Macchiavello, Phys. Rev. A **59**, 4249 (1999)
[6] J. Eisert, K. Jacobs, P. Papadopoulos, and M. B. Plenio, Phys. Rev. A **62**, 052317 (2000)
[7] M. A. Nielsen and I. L. Chuang, Phys. Rev. Lett. **79**, 321 (1997)
[8] A. S. Sørensen and K. Mølmer, Phys. Rev. A **58**, 2745 (1998)
[9] D. Collins, N. Linden, and S. Popescu, Phys. Rev. A **64**, 032302 (2001)
[10] Y.-F Huang, X.-F Ren, Y.-S. Zhang, L.-M. Duan, and G.-C Guo, Phys. Rev. Lett. **93**, 240501 (2004)
[11] G.-Y Xiang, J. Li, G.-C. Guo, Phys. Rev. A **71**, 044304 (2005)
[12] S. F. Huelga, M. B. Plenio, G.-Y. Xiang, J. Li, and G.-C Guo, quant-ph/0509057
[13] D. M. Greenberger, M.A.Horne, and A.Zeilinger, in Bells Theorem, Quantum Theory, and Conceptions of the Universe, edited by M. Kafatos (Kluwer Academic, Dordrecht, 1989), pp.73-76; D. M. Greenberger, M. A. Horne, A. Shimony, and A. Zeilinger, Am.J.Phys. **58**,1131 (1990)
[14] A. Karlsson and M. Bourennane, Phys. Rev. A **58**, 4394 (1998)
[15] C.-P. Yang, S.-I Chu, and S. Han, Phys. Rev. A **70**, 022329 (2004)
[16] F.-G. Yang, C.-Y. Li, H.-Y. Zhou, and Y. Wang, Phys. Rev. A **72**, 022338 (2005)
[17] M. Hillery, V. Bužek, and A. Berthiaume, Phys. Rev. A **59**, 1829 (1999)
[18] W. K. Wootters and W. H. Zurek, Nature (London) **299**, 802 (1982)
[19] H.Barnum, C. M. Caves, C. A. Fuchs, R. Jozsa, and B. Schumacher, Phys. Rev. Lett. **76**, 2818 (1996)
[20] M.A. Nielsen, I.I. Chuang, Quantum Computation and Quantum Information(Cambridge University Press, 2000)
[21] Liang Qiu and An Min Wang, unpublished